



“Analyzing Metadata from Offline Phishing Scams”

Presented by

Mark Henderson

Internal Revenue Service

Privacy, Information Protection & Data Security

Online Fraud Detection & Prevention

Learning objectives

Attendees should be able to describe:

- different IRS online/offline scams
- various tools/techniques to extract metadata from files (text, PDF, images)
- open-source tools to visualize data
- techniques to reveal relationships within data
- ways to detect/mitigate offline phishing scams

What is PIPDS?

- PIPDS preserves and enhances public confidence of the IRS by advocating for the protection and proper use of identity information
- Established July 2007, PIPDS ensures security of IRS systems and proper protection of personal information
- Two main offices deliver four main programs
 - PIP (Privacy and Information Protection)
 - Privacy (UNAX, SSN E/R, PIAs)
 - Identity Protection
 - Incident Management
 - OFDP (Online Fraud Detection & Prevention)
- Promote protecting information through education and awareness

Who am I?

- Started IT career in GSM fraud
- Worked in subpoena compliance/internet abuse/customer router security at UUNet
- Worked as analyst/security engineer at US-CERT for several years
- Joined IRS Online Fraud in 2009

What is OFDP's mission?

“To reduce online fraud against the IRS and taxpayers working closely with public, private and international stakeholders.”

What do we investigate?

- Falsely purport to be the IRS
- Falsely purport to be an authorized agent or partner of the IRS
- Falsely assert to conduct business on behalf of the IRS
- Falsely claim to be an authorized Electronic Return Originator (ERO) for the purposes of fraudulently obtaining tax return information, and/or
- Unlawfully display or misuse IRS logos in violation of Title 31, United States Code, Section 333 (Prohibition of misuse of Department of the Treasury names, symbols, etc.)

Why?

- The manner in which the IRS handles phishing is a key factor in the continued success of e-Gov initiatives
- As the IRS continues to modernize its infrastructure any loss of taxpayer confidence undermines this strategy and its investments

IRS Scams in 10 minutes

OFDP Responsibilities

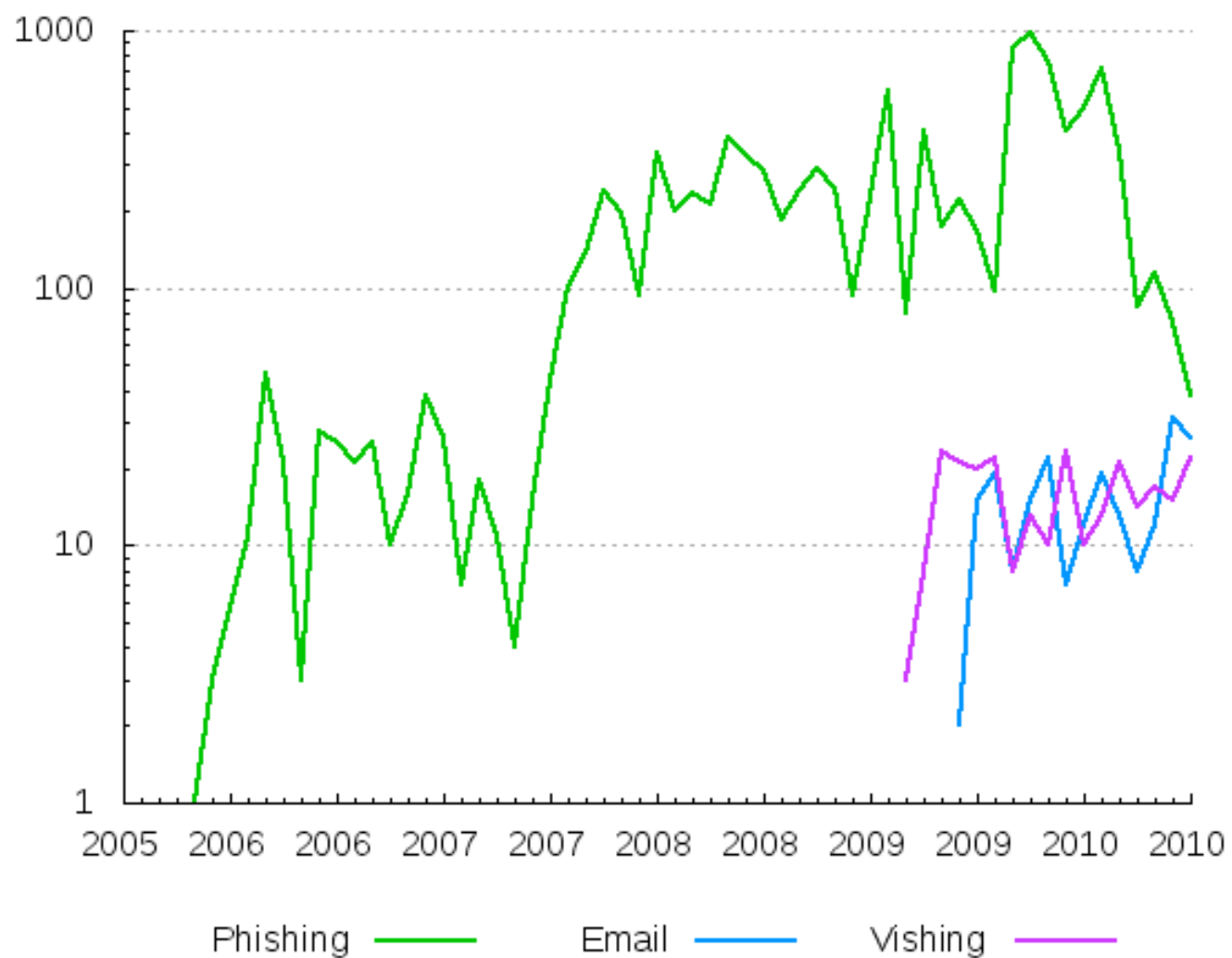
Online scams (“occurs entirely online”)

- Phishing websites
- Fraudulent efile/unauthorized efile
- Misrepresentation online (e.g., Facebook)

Offline scams (“online receipt, offline response”)

- Vishing (voice + phishing)
- Email (Stock*, “Funds Transfer”, Lottery)

OFDP Incident Statistics



Phishing

- Primary focus of OFDP (phishing@irs.gov)
- Fake IRS websites advertised through emails that include malicious URLs or attachments
- Phishtank listed IRS as #2 most targeted brand in Feb 2010, second only to Paypal
- Most technically challenging
- Beginning in September 2009 and into 2010 a large-scale, botnet-driven malware campaign (Avalanche/Zeus) targeted the IRS as well as others
 - 2005-2008 ~4000 incidents, 2009 ~5000 incidents (~4100 botnet-related)



Internal Revenue Service

United States Department of the Treasury

[Contact IRS](#) | [About IRS](#) | [Site Map](#) | [Español](#) | [Help](#)

Keyword/Search Terms
[Advanced Search](#) [Search Tips](#)

[INDIVIDUALS](#) | [BUSINESSES](#) | [CHARITIES & NON-PROFITS](#) | [GOVERNMENT ENTITIES](#) | [TAX PROFESSIONALS](#) | [RETIREMENT PLANS COMMUNITY](#) | [TAX EXEMPT BOND COMMUNITY](#)

Most Requested Forms and Publications

1. [Form W-4](#)
2. [Form W-9](#)
3. [Form 1040](#)
4. [Form SS-4](#)
5. [Form 8822](#)

[More Forms and Publications](#)

Online Tools

- [Online EIN Application](#)
It's fast and user-friendly
- [Where's My Refund?](#)
It's quick, easy and secure
-  **e-file**
Fast, Easy & More Accurate.
-  **electronic IRS**
File, Pay... and More.

[More Online Tools](#)

Get Refund on your Visa or Mastercard

Please enter your information in the form below where refunds will be made.

Note: Double check your data before submitting this form.

* Full Name:

* Address:

* City:

* State:

* Postal Code:

* Phone:

* Date Of Birth: (mm/dd/yyyy)

* Social Security Number:

* Mother's Maiden Name:

* Card Number:

* Expiration Date: Month Year

* CVV / CSC: [Help finding your CVV?](#)

* Electronic Signature: (ATM PIN)

* Issuing Bank of your Credit Card:

* Bank Phone:

* E-mail:

Refund amount: \$165.01

* Required fields.

When you visit the IRS website, we collect your IP address and standard web log information, such as your browser type and the pages you accessed on our website. Before permitting you to use our Service, we may require you to provide additional information we can use to verify your identity or address or manage risk, such as your date of birth, social security number or other information. We may also obtain information about you from third parties such as credit bureaus and identity verification services. When you are using our Service, we may collect information about your computer or other access device for fraud prevention purposes.

I need to...

<Select One>



td>

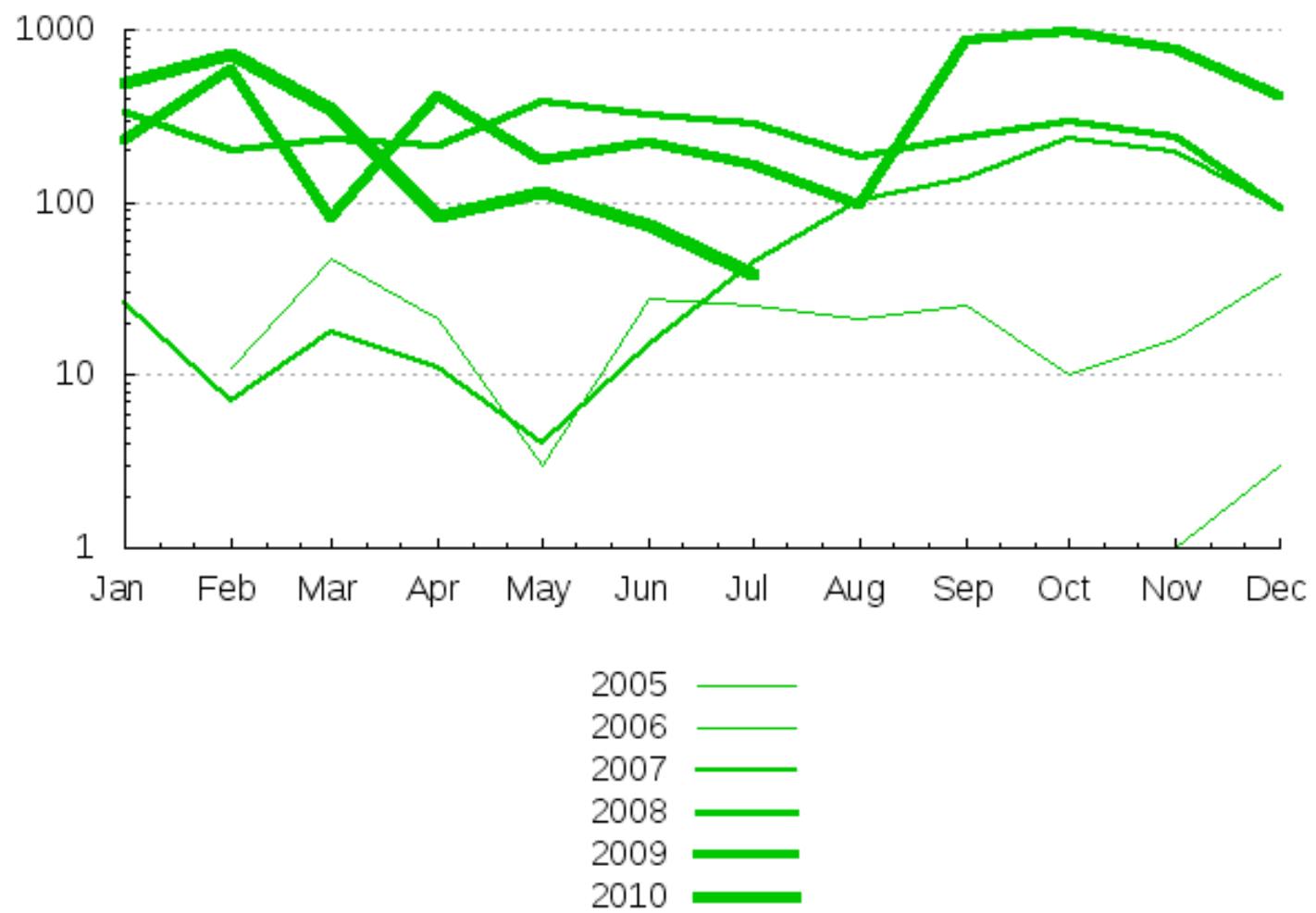
NEW e-file for Excise Taxes

Is your Form 2290 due?
Why not e-file!

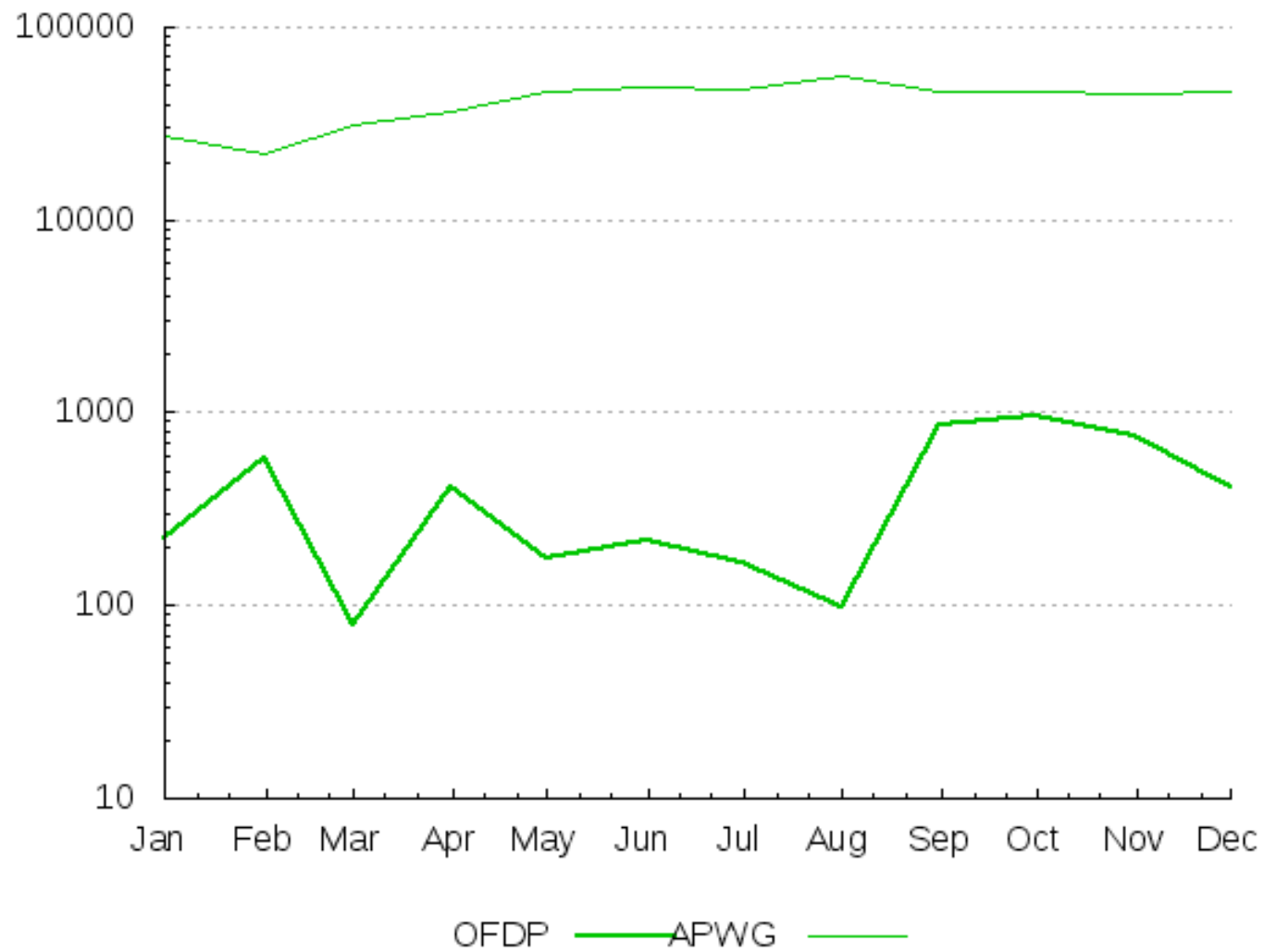
BONUS at Anaheim Forum

Multicultural issues? Talk to experts. Sept 13, 8am-1:30pm.

OFDP Offline Phishing (Phishing)
Comparison 2005 to Present



OFDP/APWG Phishing Statistics [2009]



Fraudulent/unauthorized e-file

- Sites that appear to be legitimate efile sites that harvest credentials
- File victim's return then collect their refund
- All but eliminated in 2009 after introduction of EV SSL certificates



HR-Prep.com



Home

Start your return

Forms supported

Tax services

FAQ

Privacy policy

Contact



ABOUT FREE FILE

The speed, accuracy, and convenience of computers allow e-filed returns to be processed faster and more accurately than paper returns. You can e-file your return from home or through a tax professional using an authorized software package anytime of the day or night.



Prepare your 2005, 2006, or 2007 tax return online

We provide you with expert advice and free live support. Whatever your tax situation, customer satisfaction is our #1 priority. You can file late at HR-Prep.com.

Do you Owe the IRS?

We realize that being past due on your taxes may make you feel uneasy. Have peace of mind and prepare an IRS INSTALLMENT PLAN online. You can also have a tax professional review your return and if needed, represent you before the IRS.

Are You Getting a Refund?

The U.S. Treasury still has billions of dollars of unclaimed tax refunds. Prepare your return today to uncover how much is waiting for you. If you are getting a refund, you are usually still required to file a tax return. Let us help you get this done quickly and file your past year tax return online.

Did you need a copy of your prior year (2002 - 2007) tax return or a supplemental form (W2, 1099-R) that was already filed with the IRS?

If you filed your prior or current year tax return, you can request the IRS transcripts of your tax return, W2, or 1099-R and receive it on the SAME BUSINESS DAY (if requested before 3 PM EST).

Completing the request only takes 5 minutes, and the IRS authorized transcripts are good for Mortgages, Student Loans, Legal Documentation, etc.

It's fast, it's easy,
it's simply the best way to file...

FREE REFUND CALCULATION

User Name:

Email Address:

SUBMIT

Start a new
Tax Return
NOW!

START A NEW RETURN

Your Federal tax return is guaranteed accurate. Easy to use, user-friendly interface. Free federal e-file \$9.95 optional state return

[more information...](#)

CONTINUE YOUR RETURN

You do not have to complete your entire return at one time. You can start your return, stop and come back as many times as you need to finish your return.

[more information...](#)

CHECK E-FILE STATUS

Receive a refund in about half the time as a paper filer with e-file!

[more information...](#)



[Home](#) | [Start your return](#) | [Forms supported](#) | [Tax services](#) | [FAQ](#) | [Privacy policy](#) | [Contact](#)

Copyright © 2008 HR-Prep.com. All rights reserved.

Misrepresentation

- Companies that display an efile logo that are not registered efilers
- Group pages created on Facebook purporting to be affiliated with the IRS



Department of the Treasury
Internal Revenue Service

Suggest to Friends

The IRS Mission:
Provide America's taxpayers top quality service by helping them understand and meet their tax responsibilities and by applying the tax law with integrity and fairness to all.

Information

Location:
1111 Constitution Ave., NW
Washington, DC, 20224

Phone:
1-800-829-1954

Fans

6 of 66 Fans

See All



Johnny R. Hite



Renee Williams



Steve Shanty



Caleb Mustafa



David Korshberg



Andrew Prihar

Links

2 links

See All

IRS e-file: It's Safe; It's Easy; It's Time
10:11pm Feb 25

ETC Home Page--It's easier than ever to find out if you qualify for ETC
10:10pm Feb 25

Internal Revenue Service (The IRS)

Become a Fan

Wall Info Photos Discussions

Internal Revenue Service (The IRS) + Fans **Internal Revenue Service (The IRS)**
Just Fans



Internal Revenue Service (The IRS)
<http://www.irs.gov/newsroom/article/0,,id=218319,00.html?portlet=7>

IRS e-file: It's Safe; It's Easy; It's Time
www.irs.gov

Videos: E-File Director's Message: English | SpanishFree File and Fillable Forms: English | Spanish | ASLAsk Your Tax Preparer to e-File: EnglishFirst Time Filing a Tax Return? EnglishFile and Direct ...

February 25 at 10:11pm · Share



Internal Revenue Service (The IRS)
<http://www.irs.gov/individuals/article/0,,id=96406,00.html?portlet=7>

ETC Home Page--It's easier than ever to find out if you qualify for ETC:
www.irs.gov

The Earned Income Tax Credit or the EITC is a refundable federal income tax credit for low to moderate income working individuals and families. Congress originally approved the tax credit legislation in 1975 in part to offset the burden of social security taxes and to provide an incentive to work. ...

February 25 at 10:10pm · Share



Internal Revenue Service (The IRS) The IRS spent just 44 cents for each \$100 it collected in 2005.

February 25 at 9:29pm



Internal Revenue Service (The IRS) The IRS is a bureau of the Department of the Treasury and one of the world's most efficient tax administrators. In 2004, the IRS collected more than \$2 trillion in revenue and processed more than 224 million tax returns.

February 25 at 9:29pm

RECENT ACTIVITY

Internal Revenue Service (The IRS) edited their Phone, Location and Website.

Internal Revenue Service (The IRS) joined Facebook.

Internal Revenue Service (The IRS) has no more posts.

Create an Ad

Your City, Your Rules ✕



Be the mayor in SocialCity and construct a bustling city. Play now!

Like

What is that? ✕



...a Gremli! See what other crazy animals are waiting for you in Zoo World!

Like

Bored? Kill Some Time ✕



Join millions of others. Your friends have. Show them who is boss. Click here to play Mafia Wars.

Like

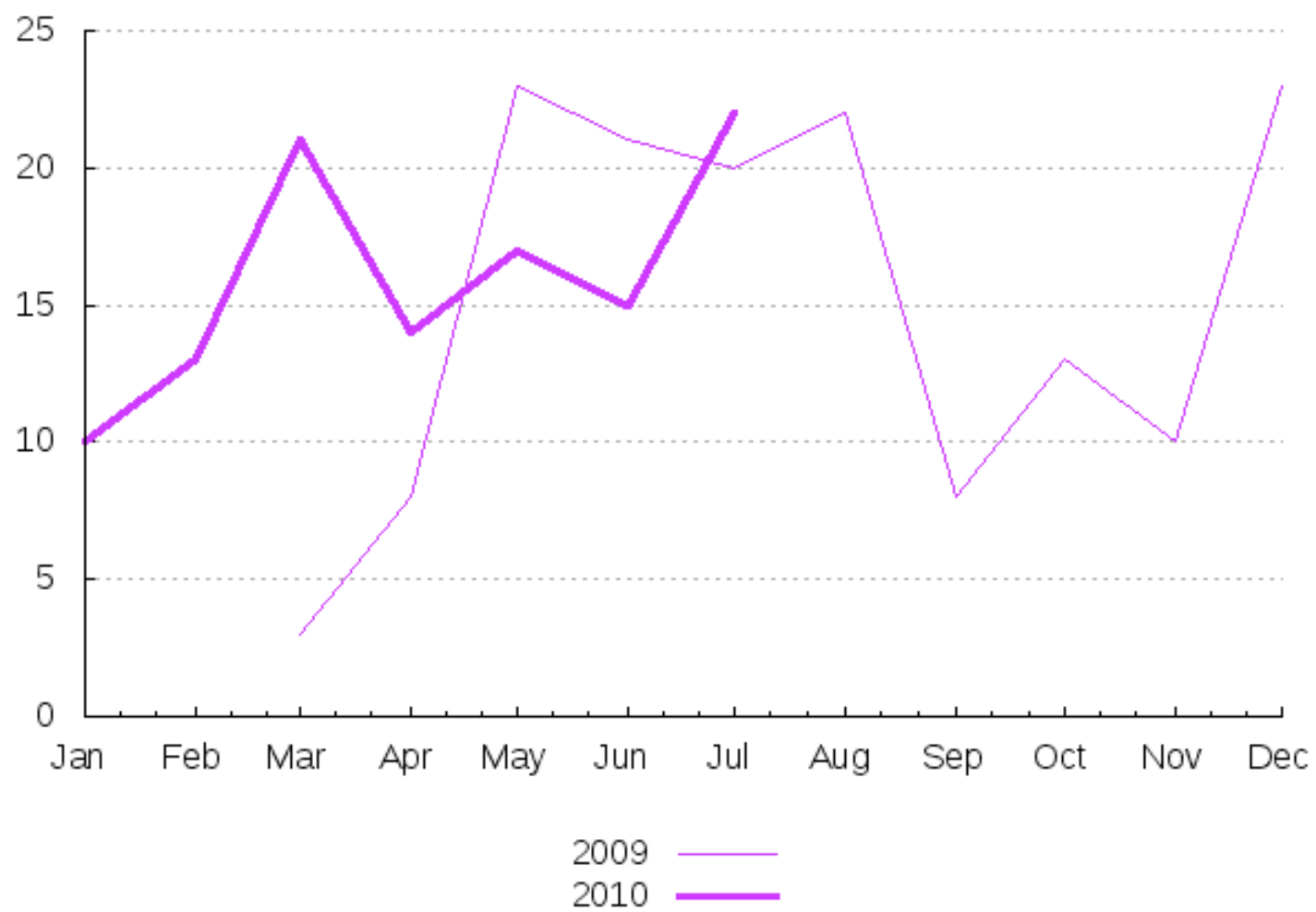
More Ads

Create a Page for My Business
Report Page

Vishing

- Seen since at least 2002
- ~10-15 month
- W-8BEN most popular fake IRS form
- Predominantly one telco is used
- Recipients often OCONUS but telco providers in US
- Have observed other agencies being used

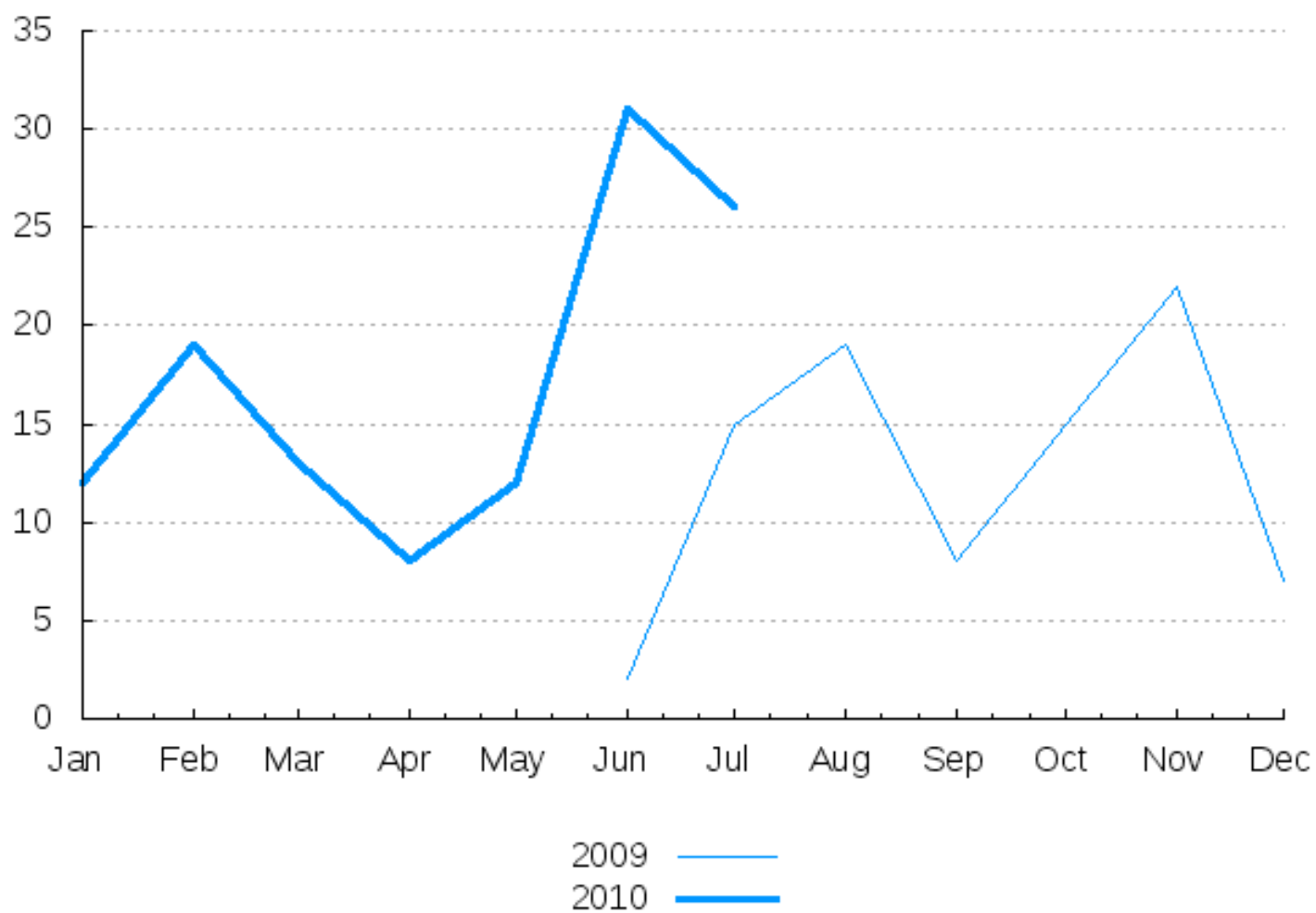
OFDP Offline Phishing (Vishing)
Comparison 2009 vs 2010



Email

- Began with attempt to track scams using the Treasury Secretary (Geithner)
 - Evolved into any scam using email addresses linked to the IRS/Treasury
- ~20 to 30 a month
- Bulk of email scams simple spam but also track emails from stock and vishing scams
- Intl. phone numbers prefixes usually can give you an idea of where scam originates
- Have observed other agencies being used

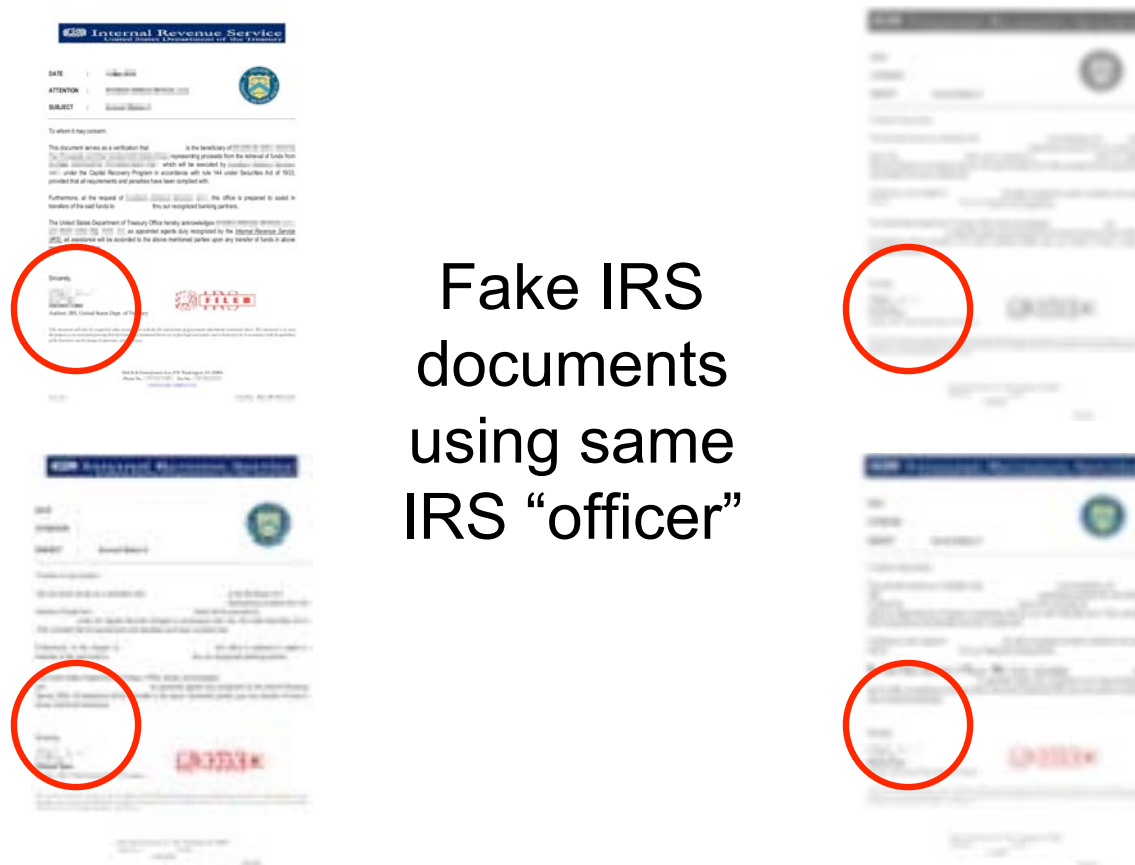
OFDP Offline Phishing (Email)
Comparison 2009 vs 2010



Stock

- Elaborate scams involving telephone calls, emails, fake websites, mirrored content, fake documents
- Likely boiler-room operation operated overseas
- ~10% of all vishing numbers investigated
- High loss ratio (\$2K - \$200K)
- Almost exclusively foreign victims
- Have observed other agencies being used

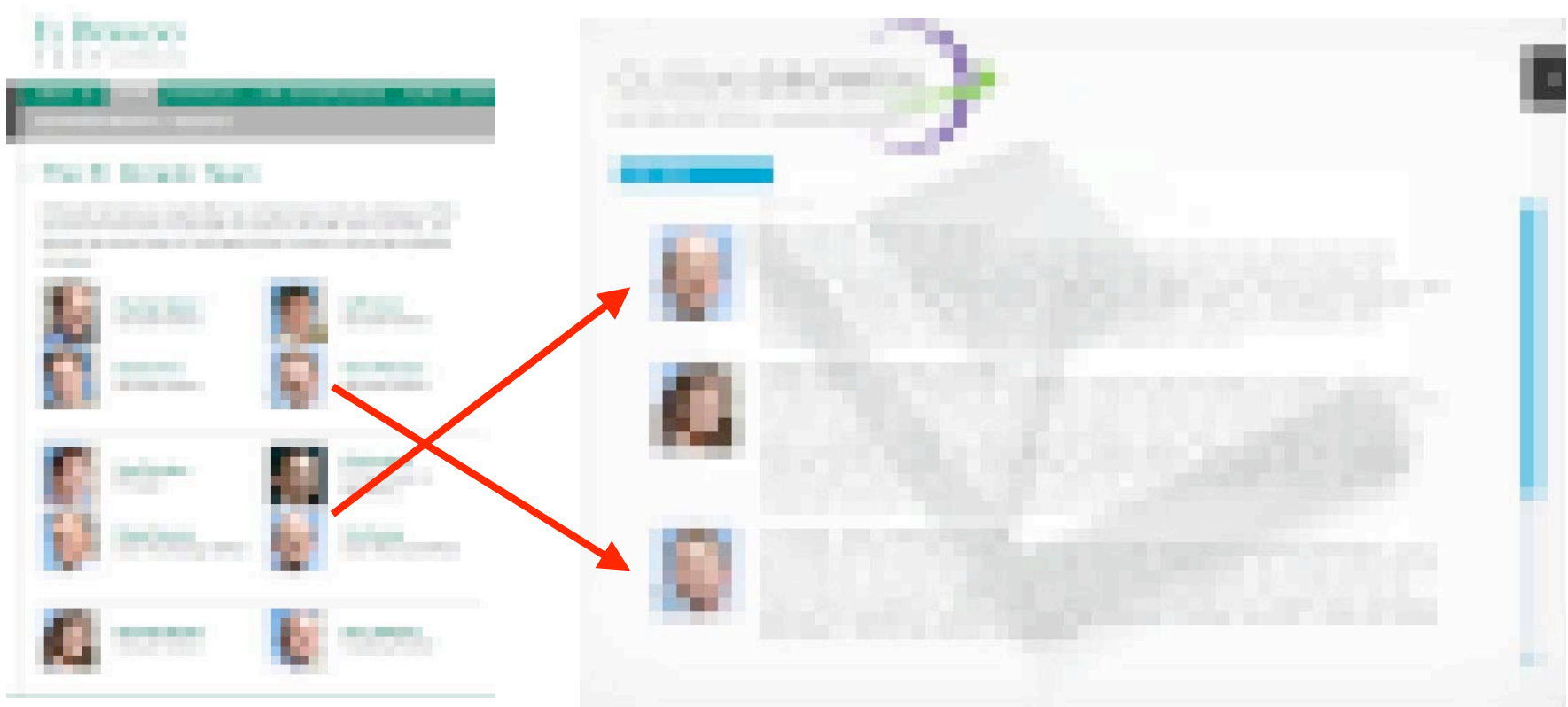
Stock scam (documents)



Stock scam website (swap)

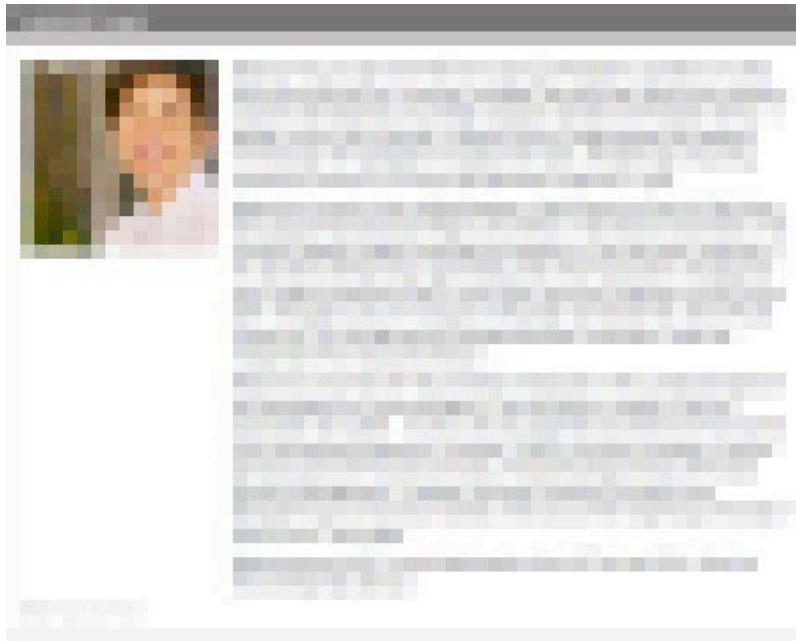
REAL

FAKE

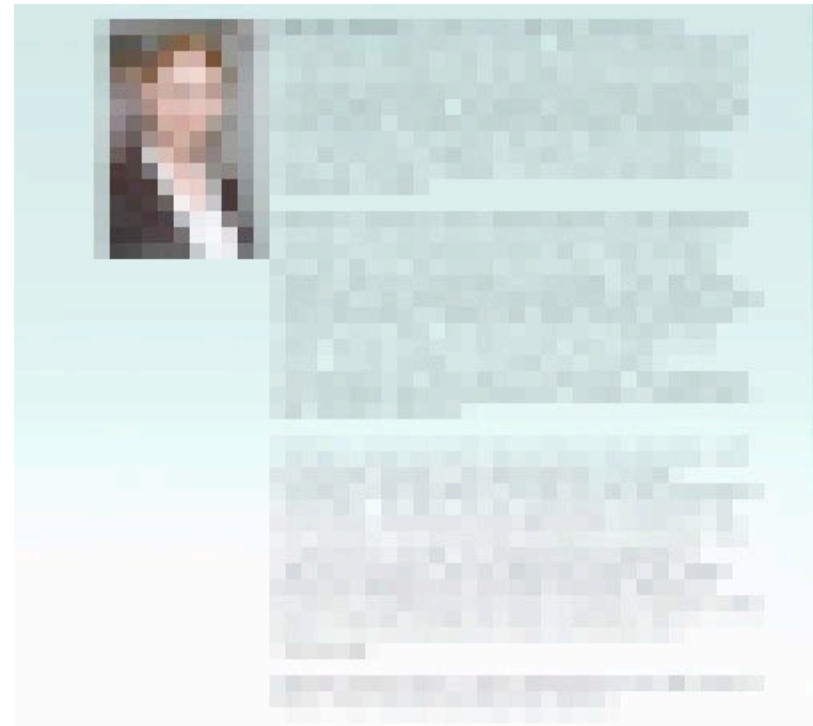


Stock scam website (replace)

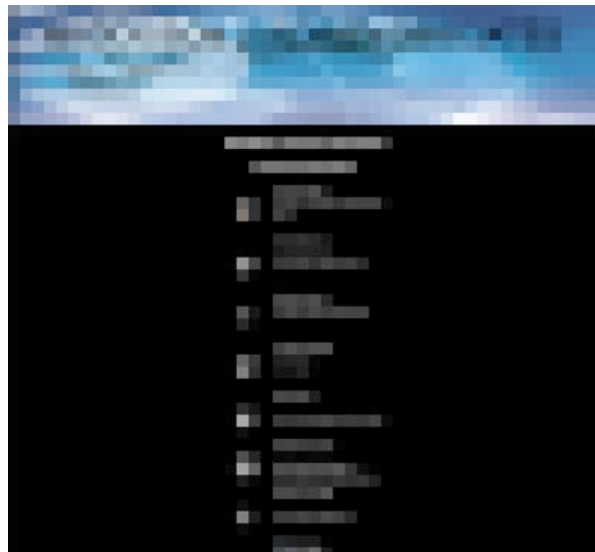
REAL



FAKE



Stock scam clones



Clone #1



Clone #2

Original scam site

"Funds Transfer"/Lottery

- Basic advance fee scam
- <5% of incidents
- Mostly conducted via email (spam) but in some cases tailored to individual
- Have observed other agencies being used

Funds Transfer



NEW YORK (Hartem), 55 W. 125th. Monday – Friday 8:30 a.m. – 4:30 p.m.
TEL/FAX: Email: usairsrev

OUR REF: US/IRS/KC-2010. DATE: 30th JUNE 2010.


- * Account inquiries (help with letter, notices and notices on your wages or bank account)
- * Address it changes to the account information to payments.
- * Ask a Clearance (Calling Payment)
- * Application for Taxpayer Assistance Order (TAO)
- * Copies of Tax Returns & Transcript (usually available for current year and three prior years)
- * Help with preparing Form 2250 (de any income tax)
- * Multilingual Assistance over 150 languages translated
- * Payment Payment Management
- * Pre-identification
- * Continue to Tax Issues
- * Tax Forms (based on availability)
- * Tax Law Assistance (also available to your Individual Federal Tax Return)
- * (On call)
- * Taxpayer Identification Number

URGENT STOP ORDER:

ATTN:
(PRESIDENT-STANDARD CHARTERED BANK, NEW YORK).


SIR,

IT HAS COME TO OUR NOTICE THROUGH OUR INTELLIGENT MONITORING UNIT THAT, YOU HAVE CONCLUDED THE FULL ARRANGEMENT OF TRANSFERRING FUNDS VALUED US\$1.5 MILLION IN FAVOR OF ONE OF KUWAIT, ON HIS ACCOUNT WITH: Account Name:





THIS IS IN LINE WITH THE FINANCIAL POLICY NEWLY AMENDED BY OUR PRESIDENT OBAMA THAT ANY SINGLE DOLLAR PAYMENT THAT BELONG TO THE AMERICANS MUST OBTAIN A TAX CLEARANCE CERTIFICATE BEFORE A FINAL CREDIT IS MADE TO THE BENEFICIARY'S ACCOUNT.

AT THIS JUNCTURE, WE STOP THE FURTHER REMITTANCE OF THIS FUND TILL THE BENEFICIARY PROCURES HIS TAX CLEARANCE CERTIFICATE TO THIS EFFECT, WHICH HAS BEEN CALCULATED FROM 2009/2010 ANNUAL TAX FEE OF US\$30,000.00 ONLY. PLEASE YOU ARE REQUIRED TO MAKE THIS PAYMENT THROUGH OUR RECEIVING AGENT ACCOUNT AS STATED BELOW:



YOURS FAITHFULLY



MR. BOBBY WHEELER
(DIRECTOR, INLAND REVENUE SERVICES).

CC:FBI UNITED STATES.
CC:INTERPOL LONDON.
CC:BARACKS OBAMA,WHITE HOUSE,WASHINGTON DC.
CC:INTERNATIONAL FINANCIAL REGULATORY USA.

Lottery

P1.4 Notification form



Name _____
Address _____
City _____ State _____ County _____
E-mail _____
Telephone _____
Date of Birth _____ Country of Birth _____ Country _____
Number of dependents _____
Do you owe any back Taxes? Yes _____ No _____
Are Currently Employed? Yes _____ No _____
Have you ever been convicted of a criminal act? Yes _____ No _____
*If yes please state the nature of the offence _____

Do you have a valid Government issued ID? Yes _____ No _____
What amount of money are you expecting to carry into this country _____

*I _____ (Please print name) guarantees that all the above information is true and correct and understands that any false information will lead to my prize money being barred from entering the country.
Signature of Applicant _____ Date _____
Signature of Remittance Co. _____ Date _____
Signature Agent (IRS) _____ Date _____



With Over 20-Years Experience,
We Make Sweepstakes Effective, Simple & Fun!

AMERICAN SHOPPERS Network



RESULTS FOR FIRST (1st) CATEGORY DRAWS

Congratulations to you as we bring to your notice, the results of the Grand Prize Category draws of US Sweepstakes And Fulfillment Company. We are happy to inform you that you have emerged a winner under the First Category, which is part of our promotional draws. Participants were selected through a computer ballot system drawn from 15,000,000 names of individuals from America, Canada, and Europe, as part of our International Promotions Program.

Your name _____ with prize number 1008 for the multi-million dollar sweepstakes, and consequently won the First Place Prize.

You have therefore been awarded a total sum pay out of **US\$15,500,000.00** (fifteen Million Five Hundred Thousand United States Currency). This is from the total prize money of US\$35,000,000.00 shared among the three (3) international winners.

CONGRATULATIONS!

Your fund is now deposited with "Wachovia Bank" insured in your name. For your own security reasons you are been advised to keep your winning information; i.e Reference, Transfer, Tracking Numbers, I.D. Cards confidential and in a safe place until you have claimed your prize and your funds remitted to your account. This is part of our security protocol to avoid double claiming or unscrupulous acts by participants / non participants of this program.

Due processing and remittance of your prize money to a designated account of your choice Remember, you must contact your Agent. NOTE: In order to avoid unnecessary delays and complications, please remember to quote your reference number arising from your *Western Union Money Transfer, Money Gram or a Manager's cashiers Cheque* in respect of your *Security Deposit* to expedite this process. Furthermore, in the event where there are any change of your address / contact number; please inform your claims agent as soon as possible.

We also wish to bring to your attention our New Year high stakes where you stand a chance of winning a European Sports Car, value up to US\$375,000.00 we hope that with a part of your prize you will participate. Please contact me at anytime for any further questions. See copy of your check below for your case of reference.

Notice: To collect your original copy of the Cheque please pay all the necessary taxes.

Thank you, for entering the sweepstakes.



©2004 US SWEEPSTAKES & FULFILLMENT CO. 625 PA

G 2, SUITE 100, PO BOX 25-07, ROCHESTER, NY 14609



We have not yet received payments on your IRS Tax & US
g Fee, Delivery fee, Wire Transfer and your Stamp of
from the American Shoppers Network Sweepstakes

For more information please do not hesitate to contact the undersigned.

Payment Scheme

-	\$ 000
-	\$ 000
-	\$ 000
-	\$000
-	\$000
-	\$000

End result the same ...

- OFDP contacts {registrar, registrant, hosting provider, carrier}
 - Domain de-registered
 - Content removed
 - Email address suspended
 - Fax number disabled

Offline phishing

Why do they fax?

- no extra telephone line required for the fax
- paperless communication, integrated with email
- send and receive multiple faxes simultaneously
- reduction in phone costs
- ability to receive and send faxes from any location that has Internet access

[Source: Wikipedia]

How do they do it?

- Send out spam listing a fax number or send a direct fax
- Use free email accounts to send out fake IRS forms
 - Even if account is disabled it served its purpose; response doesn't go back to same email
- Use free fax services to receive faxes
- Free fax services can forward the fax to same/diff email account

Vishing - Email

- Most commonly received as an attachment to an email
- Sometimes multiple fax #s are provided or a fax # and an email
- Multiple forms used but follow same basic format
- Metadata often available
- Sometimes they change the numbers in the email but not in the actual document

Vishing (email)

Sir/Madam,

Our records indicate that you are a Non-resident. As a result you are exempted from United States of America Tax reporting and withholdings on interest paid to you on your account and other financial benefits.

To protect your exemption from tax on your account and other financial benefits, you need to recertify your exemption status and enable us confirm your records with us.

Therefore, you are to authenticate the following by completing form W-8BEN and return to us as soon as possible through fax numbers [REDACTED] OR [REDACTED]

When completing form W-8BEN, please follow the steps below:

1. We need you to provide your permanent address if different from the current mailing address.
2. You must indicate as a Non-US resident, the country you are residing, to support your non-resident status and if your bank or other financial institutions you are dealing with has a US address for mailing purposes.
3. If any joint account holder is now a US resident or citizen, or in any way subject to US tax reporting laws: please check the box in this section.
4. Please complete 1 through 19 and have all account holder/s (if more than one account holder) sign and date the form separately and fax to the above-mentioned fax numbers.

Please complete Form W-8BEN (attached) and return to us with one week from the receipt of this letter by faxing it, to enable us confirm your records immediately.

If your records are not confirmed on time, you will lose your Non-resident status tax exempt benefits and your account or any other financial benefits will be subject to US tax reporting and back up withholding*

*If back up withholding applies, we are required to withhold 30% of the interest/benefits paid to you.

We appreciate your cooperation in helping us protect your exempt status and also confirm our records.

Sincerely,

Marlie Parks,

IRS Public Relations.

Vishing (attachment)

Form W-4100B2 is very similar to W8-BEN form

Form W-4100B2

To make an application to receive interest with no U.S. tax taken off
Interest on U.S. government securities, bonds, and other deposits taken. They will arrange for interest to be paid without tax taken off.

PART 1: IDENTIFICATION OF BENEFICIAL OWNER(S)

Surname and Title:		Other name(s):		Sex:	
Nationality:	Date of Birth:	Place of Birth:	Town/City:		
Mother's maiden Name:	U.S. Social Security No.:		Passport Number:		
		Employer Number:			
Occupation/Profession:	Name of Employer:		Address of Employer:		
Name of Bank:	State Account Number:		Date Account was opened:		
Branch Address:			Routing #:		
Membership/Club ID Number:			Debit/Credit Card #:		Renewable Debit/Credit Card #:
Any other Bank Account:	Account Number:	Date Account was opened:		Routing #:	
Country of Permanent Residence (if other than place of birth):					
Home Telephone Number:		Office Telephone Number:		Mobile Telephone Number:	
Full Residential Address:			Full Mailing Address:		
Full Residential Address:					
How often do you visit the country: () Regularly () Occasionally ()			When was your last visit:		
State your intention to return (amount and length stay):			Which of the following is your primary residence of: () Home () Telephone () Any other (specify):		

PART 2: CERTIFICATE

UNDER PENALTY OF PERJURY, I/We hereby certify that the information on this form is true, correct and complete.

PART 3: SIGNATORIES

Signature	Name	Date of Birth
Signature	Name	Date of Birth

Vishing - Direct fax

Fax header

- # faxed from
- can identify visher's name and/or FoIP provider

Internal Revenue Service IRS.gov
DEPARTMENT OF THE TREASURY
JULY, 2010

THE ACCOUNT HOLDER(S)

Our records indicate that you are a non-resident alien. As a result, you are exempted from United States of America Tax reporting and withholdings on interest paid on your account and other financial dealing to protect your exemption from tax on your account and other financial benefit in rectifying your exemption status.

Therefore, you are to authenticate the following by completing form W-8BEN, and return to us as soon as possible through the fax number: [redacted]
If you are a USA Citizen and resident, please indicate "USA Citizen/Resident" on the form and return it to us. We shall also update your record as the law permits us.

When completing form W-8BEN, please follow the steps below

1. We need you to provide your permanent address if different from the current mailing address on your Form W-8BEN. If you are a non-USA resident, you must indicate if a non-USA resident, your country of origin to support your non-resident status (if your bank account or other financial dealing has a USA address for mailing purpose).
2. If any joint account holder are now USA residents or Citizen, or in any way subject to USA tax reporting laws, Please check the box in this section.
3. Please have all account holders, sign and date the form separately and fax it to the above-mentioned number.

Please, complete Form W-8BEN "attached" and return to us within 1 (one) week from the receipt of this letter by faxing it, to enable us update your records immediately if your account or any other financial benefits are not rectified in a timely manner, it will be subject to USA tax reporting and back up withholding (if back up withholding applies, we are required to withhold 30% of the interest paid to you).

We appreciate your cooperation in helping us protect your exempt status and also update our records.

Sincerely,
[Signature]
Director of Information

Three fax numbers

Person referenced

Email vs. Direct Fax

FORM W-8BEN (NRA Recertification) Request for Recertification of Foreign Status (NOVEMBER, 2009)

W-8BEN (Substitute form)		Certificate of Foreign Status of Beneficial Owner For United States Tax Withholding	
Part I Identification of Beneficial Owner			
1. Name of individual or organization that is the beneficial owner		2. Sex: <input type="checkbox"/> male <input type="checkbox"/> female	
3. Type of beneficial owner		<input type="checkbox"/> Individual <input type="checkbox"/> Corporation <input type="checkbox"/> Complex Trust <input type="checkbox"/> Simple Trust <input type="checkbox"/> Grantor Trust <input type="checkbox"/> Central Bank of issue <input type="checkbox"/> Government <input type="checkbox"/> International organization <input type="checkbox"/> Tax-exempt organization <input type="checkbox"/> Private foundation	
4. Date of Birth			
5(a). Nationality:		5(b). Place of Birth:	
6(a). Country of permanent Residence		6(b). Passport Number:	
7. Mothers Maiden Name:			
8(a). Spouse Name:		8(b). Spouse date of Birth:	
9. Permanent resident address (street, apt, or suite no, or rural route). Do not use a P.O. box or in-care of address			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
10. Mailing address (if different from above)			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
11. Social Security Number (if any)		<input type="checkbox"/> SSN or ITIN <input type="checkbox"/> EIN	
12. Profession:		13. Day time phone/ fax Number	
14.(a) Bank Name(s): *(US BANKS ONLY) *			
15. Account number(s)/Account names:			
16. Branch Address:			
17. Date Account(s) was opened:			
18. How often do you come to USA and when did you arrive last?			
19. ATTACH PHOTOCOPY OF PASSPORT FOR PROPER IDENTIFICATION			
Part II Certification of Beneficiary Owner			
Under penalties of perjury, I declare that I have examined the information on this form to the best of my knowledge and believe it is true, correct and complete. I further certify under penalties of perjury that:			
<ul style="list-style-type: none"> I am the beneficial owner (or am authorized to sign for the beneficial owner) of all the income to which this form relates. The beneficial owner is not a U.S. person. The income to which this form relates is not effectively connected with the conduct of a trade or business in the United States or is effectively connected but subject to tax under an income tax treaty, and For broker transaction or better exchanges, the beneficial owner is an exempt foreign person as defined in the instructions. 			
Furthermore, I authorized this form to be provided to any withholding agent that has control, receipt or custody of the income of which I am the beneficial owner or withholding agent that can disburse or make payments of the income of which I am the beneficial owner.			
The Internal Revenue Service does not require your consent to any provisions of this document other than the Certifications required to establishing your status as a non-U.S. person and, if applicable, obtain a reduced rate of withholding.			
Sign Here (Signer #1)		Date	
Signature of beneficial owner or individual authorized to sign for beneficial owner			
Sign Here (Signer #2)		Date	
Signature of beneficial owner or individual authorized to sign for beneficial owner			

SEND TO FAX NO: [REDACTED]

FORM W-8BEN (NRA Recertification) Request for Recertification of Foreign Status FEBRUARY, 2010

W-8BEN (Substitute form)		Certificate of Foreign Status of Beneficial Owner For United States Tax Withholding	
Part I Identification of Beneficial Owner			
1. Name of individual or organization that is the beneficial owner		2. Sex: <input type="checkbox"/> male <input type="checkbox"/> female	
3. Type of beneficial owner		<input type="checkbox"/> Individual <input type="checkbox"/> Corporation <input type="checkbox"/> Complex Trust <input type="checkbox"/> Simple Trust <input type="checkbox"/> Grantor Trust <input type="checkbox"/> Central Bank of issue <input type="checkbox"/> Government <input type="checkbox"/> International organization <input type="checkbox"/> Tax-exempt organization <input type="checkbox"/> Private foundation	
4. Date of Birth			
5(a). Nationality:		5(b). Place of Birth:	
6(a). Country of permanent Residence		6(b). Passport Number:	
7. Mothers Maiden Name:			
8(a). Spouse Name:		8(b). Spouse date of Birth:	
9. Permanent resident address (street, apt, or suite no, or rural route). Do not use a P.O. box or in-care of address			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
10. Mailing address (if different from above)			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
11. Social Security Number (if any)		<input type="checkbox"/> SSN or ITIN <input type="checkbox"/> EIN	
12. Profession:		13. Day time phone/ fax Number	
14.(a) Bank Name(s): *(US BANKS ONLY) *			
15. Account number(s)/Account names:			
16. Branch Address:			
17. Date Account(s) was opened:			
18. How often do you come to USA and when did you arrive last?			
19. ATTACH PHOTOCOPY OF PASSPORT FOR PROPER IDENTIFICATION			
Part II Certification of Beneficiary Owner			
Under penalties of perjury, I declare that I have examined the information on this form to the best of my knowledge and believe it is true, correct and complete. I further certify under penalties of perjury that:			
<ul style="list-style-type: none"> I am the beneficial owner (or am authorized to sign for the beneficial owner) of all the income to which this form relates. The beneficial owner is not a U.S. person. The income to which this form relates is not effectively connected with the conduct of a trade or business in the United States or is effectively connected but subject to tax under an income tax treaty, and For broker transaction or better exchanges, the beneficial owner is an exempt foreign person as defined in the instructions. 			
Furthermore, I authorized this form to be provided to any withholding agent that has control, receipt or custody of the income of which I am the beneficial owner or withholding agent that can disburse or make payments of the income of which I am the beneficial owner.			
The Internal Revenue Service does not require your consent to any provisions of this document other than the Certifications required to establishing your status as a non-U.S. person and, if applicable, obtain a reduced rate of withholding.			
Sign Here (Signer #1)		Date	
Signature of beneficial owner or individual authorized to sign for beneficial owner			
Sign Here (Signer #2)		Date	
Signature of beneficial owner or individual authorized to sign for beneficial owner			

SEND TO FAX NO: [REDACTED]

Form W-8BEN (direct fax)

REAL

Form **W-8BEN** Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding
(Rev. February 2006)
Department of the Treasury Internal Revenue Service

Section references are to the Internal Revenue Code. See separate instructions. Give this form to the withholding agent or payer. Do not send to the IRS.

OMB No. 1545-1621

Do not use this form for:
A U.S. citizen or other U.S. person, including a resident alien individual.
A person claiming that income is effectively connected with the conduct of a trade or business in the United States.
A foreign partnership, a foreign simple trust, or a foreign grantor trust (see instructions for exceptions).
A foreign government, international organization, foreign central bank of issue, foreign tax-exempt organization, foreign private foundation, or government of a U.S. possession that received effectively connected income or that is claiming the applicability of section(s) 1152, 501(c), 892, 895, or 1443(b) (see instructions).
Note: These entities should use Form W-8BEN if they are claiming treaty benefits or are providing the form only to claim they are a foreign person exempt from backup withholding.
A person acting as an intermediary.
Note: See instructions for additional exceptions.

Instead, use Form:
W-9
W-8ECI
W-8IMY
W-8ECI or W-8EXP
W-8IMY

Part I Identification of Beneficial Owner (See instructions.)

1. Name of individual or organization that is the beneficial owner

2. Country of incorporation or organization

3. Type of beneficial owner:
☐ Individual ☐ Corporation ☐ Disregarded entity ☐ Partnership ☐ Simple trust
☐ Grantor trust ☐ Complex trust ☐ Estate ☐ Government ☐ International organization
☐ Central bank of issue ☐ Tax-exempt organization ☐ Private foundation

4. Permanent residence address (street, apt. or suite no., or rural route). Do not use a P.O. box or in-care-of address.
City or town, state or province. Include postal code where appropriate. Country (do not abbreviate)

5. Mailing address (if different from above)
City or town, state or province. Include postal code where appropriate. Country (do not abbreviate)

6. U.S. taxpayer identification number, if required (see instructions)
☐ SSN or ITIN ☐ EIN

7. Foreign tax identifying number, if any (optional)

8. Reference number(s) (see instructions)

Part II Claim of Tax Treaty Benefits (if applicable)

9. I certify that (check all that apply):
a ☐ The beneficial owner is a resident of within the meaning of the income tax treaty between the United States and that country.
b ☐ If required, the U.S. taxpayer identification number is stated on line 6 (see instructions).
c ☐ The beneficial owner is not an individual, derives the item (or items) of income for which the treaty benefits are claimed, and, if applicable, meets the requirements of the treaty provision dealing with limitation on benefits (see instructions).
d ☐ The beneficial owner is not an individual, is claiming treaty benefits for dividends received from a foreign corporation or interest from a U.S. trade or business of a foreign corporation, and meets qualified resident status (see instructions).
e ☐ The beneficial owner is related to the person obligated to pay the income within the meaning of section 267(b) or 707(b), and will file Form 8833 if the amount subject to withholding received during a calendar year exceeds, in the aggregate, \$500,000.

10. Special rates and conditions (if applicable—see instructions): The beneficial owner is claiming the provisions of Article of the treaty identified on line 9a above to claim a % rate of withholding on (specify type of income):
Explain the reasons the beneficial owner meets the terms of the treaty article:

Part III Notional Principal Contracts

11. ☐ I have provided or will provide a statement that identifies those notional principal contracts from which the income is not effectively connected with the conduct of a trade or business in the United States. I agree to update this statement as required.

Part IV Certification

Under penalties of perjury, I declare that I have examined the information on this form and to the best of my knowledge and belief it is true, correct, and complete. I further certify under penalties of perjury that:
1 I am the beneficial owner (or am authorized to sign for the beneficial owner) of all the income to which this form relates.
2 The beneficial owner is not a U.S. person.
3 The income to which this form relates is (a) not effectively connected with the conduct of a trade or business in the United States, (b) effectively connected but is not subject to tax under an income tax treaty, or (c) the partner's share of a partnership's effectively connected income, and
4 For broker transactions or barter exchanges, the beneficial owner is an exempt foreign person as defined in the instructions.
Furthermore, I authorize this form to be provided to any withholding agent that has control, receipt, or custody of the income of which I am the beneficial owner or any withholding agent that can disburse or make payments of the income of which I am the beneficial owner.

Sign Here
Signature of beneficial owner (or individual authorized to sign for beneficial owner) Date (MM-DD-YYYY) Capacity in which acting

For Paperwork Reduction Act Notice, see separate instructions. Cat. No. 250472 Form **W-8BEN** (Rev. 2-2006) Printed on Recycled Paper

FAKE

FORM W-8BEN (NRA Recertification)
Request for Recertification of Foreign Status
FEBRUARY, 2010

W-8BEN Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding
(Substitute form)

Part I Identification of Beneficial Owner

1. Name of individual or organization that is the beneficial owner 1. Sex: ☐ male ☐ female

3. Type of beneficial owner: ☐ Individual ☐ Corporation ☐ Complex Trust
☐ Simple Trust ☐ Grantor Trust ☐ Central Bank of Issue
☐ Government ☐ International organization
☐ Tax-exempt organization ☐ Private foundation

4. Date of birth 5(a). Nationality: 5(b). Place of Birth:

6(a). Country of permanent Residence 6(b). Passport Number:

7. Mother's Maiden Name:

8(a). Spouse Name: 8(b). Spouse date of Birth:

9. Permanent residence address (street, apt. or suite no., or rural route). Do not use a P.O. box or in-care-of address.
City or town, state or province. Include postal code where appropriate. Country (do not abbreviate)

10. Mailing address (if different from above)
City or town, state or province. Include postal code where appropriate. Country (do not abbreviate)

11. Social Security Number (if any)

12. Profession: 13. Day time phone/fax Number

14. (a) Bank Name(s): *(US BANKS ONLY)*

15. Account number(s)/Account name(s):

16. Branch Address:

17. Date Account(s) was opened:

18. How often do you come to USA and when did you arrive last?

19. ATTACH PHOTOCOPY OF PASSPORT FOR PROPER IDENTIFICATION

Part II Certification of Beneficial Owner

Under penalties of perjury, I declare that I have examined the information on this form to the best of my knowledge and believe it is true, correct and complete. I furthermore certify under penalties of perjury that:
1 I am the beneficial owner (or am authorized to sign for the beneficial owner) of all the income to which this form relates.
2 The beneficial owner is not a U.S. person.
3 The income to which this form relates is not effectively connected with the conduct of a trade or business in the United States or is effectively connected but subject to tax under an income tax treaty, and
4 For broker transactions or barter exchanges, the beneficial owner is an exempt foreign person as defined in the instructions.
Furthermore, I authorize this form to be provided to any withholding agent that has control, receipt or custody of the income of which I am the beneficial owner or any withholding agent that can disburse or make payments of the income of which I am the beneficial owner. I agree to update this statement as required.
The Internal Revenue Service does not require your consent to any provisions of the document other than the Certifications required to establishing your status as a non-U.S. person and, if applicable, obtain a reduced rate of withholding.

Sign Here
Signature of beneficial owner (or individual authorized to sign for beneficial owner) Date

Sign Here
Signature of beneficial owner (or individual authorized to sign for beneficial owner) Date

SEND TO FAX NO: [REDACTED]

OFDP Response

- Disabled ~250 numbers in 18 months
- Crafted an IRS audio landing page (FTC) to educate potential victims
- Worked with APWG on consumer fax initiative and coversheet
- Engaged community partners (US-CERT, APWG, CFCA, NCFTA)

WARNING!

The Fax Number You Dialed
Connects to a Scam!

You may have gotten this fax number directly via fax or from an email, text, or voicemail message.

No matter how real it seemed, it was a trick.

It's called "phishing," because scammers fish for information about you or your financial accounts. Once scammers have them, they use them to commit identity theft or fraud.

If you're concerned about your accounts, contact your financial institutions using information from your billing statement.

Learn how to protect yourself against phishing and identity theft at OnGuardOnline.gov, a website created by the Federal Trade Commission.

To learn more and see examples of fax scams please visit <http://www.antiphishing.org/resources.html#advice>

If you are located in the US, please file a complaint here: <http://www.ftccomplaintassistant.gov>

If you are located outside of the US please file a complaint here: <http://www.econsumer.gov>

APWG
www.antiphishing.org

The APWG provides this message as a public service, based upon information that the Fax number you communicated with has been involved in a phishing exploit. There is no guarantee that you have not been phished through this Fax number, or previously. This is not a complete list of steps that may be taken to avoid harm from phishing, and we offer no warranty as to the completeness, accuracy or pertinence of this advisory with respect to the page you attempted to access. Please see <http://www.antiphishing.org> for more information.

Examining metadata

Metadata

- “data about data”
- Embedded within documents and images
 - Text, PDF, Microsoft Office, Images, Flash
 - Documents
 - Author, “Last saved by”, Company
 - Images
 - date/time, geolocation, camera make/model (EXIF)
 - Flash
 - text, images, sound
- Even if absent can be created
- Goal should be to identify/record metadata then analyze to group similar incidents

Documents

- Comparison
 - Unix utilities
 - cmp,diff
 - Issue with traditional hashes
 - ssdeep (“fuzzy hashing”)
- Extraction
 - exiftool (PDF/DOC)
 - read_open_xml.pl (DOCX)

Comparison (md5)

```
$ md5 document1
```

```
MD5 (document1) =
```

```
37c4b87edffc5d198ff5a185cee7ee09
```

```
$ md5 document2
```

```
MD5 (document2) =
```

```
8fb7f402f89bbdb2ee5b2f28d5673038
```


Comparison (cmp & diff)

- Standard Unix utilities

The quick brown fox jumps over the lazy dog (document1)

The quick **red** fox jumps over the lazy dog (document2)

\$ cmp -b document1 document2

document1 document2 differ: byte 11, line 1 is 142 b 162 r

\$ diff document1 document2

1c1


< The quick brown fox jumped over the lazy dog

> The quick red fox jumped over the lazy dog

Comparison (ssdeep)

```
# ssdeep -lpva original.doc rev2.doc  
rev3.doc rev4.doc rev5.doc  
rev6.doc rev7.doc rev8.doc  
rev9.doc rev10.doc ssdeep_test.doc  
ssdeep_test_rev.doc ssdeep_fw8ben.pdf  
original.doc matches rev2.doc (80)  
original.doc matches rev3.doc (80)  
original.doc matches rev4.doc (79)  
original.doc matches rev5.doc (80)  
original.doc matches rev6.doc (83)  
original.doc matches rev7.doc (77)  
original.doc matches rev8.doc (79)  
original.doc matches rev9.doc (79)  
original.doc matches rev10.doc (79)  
original.doc matches ssdeep_test.doc (0)  
original.doc matches ssdeep_test_rev.doc (0)  
original.doc matches ssdeep_fw8ben.pdf (0)
```

Documents
with slight
changes show
high similarity
(~80%)



Legitimate form
is not similar



exiftool

```
$ exiftool FORM\ W-8BEN.doc
ExifTool Version Number      : 7.69
File Name                    : FORM W-8BEN.doc
File Size                    : 51 kB
File Modification Date/Time   : 2010:01:03 13:26:32-06:00
File Type                    : DOC
MIME Type                    : application/msword
Title                       : FORM W-8BEN (NRA Recertification)
Author                      : ALPHA
Template                     : Normal
Last Saved By                : BRAVO
Revision Number              : 23
Software                     : Microsoft Office Word
Total Edit Time               : 1.0 days
Last Printed                 : 2006:09:05 15:54:00
Create Date                  : 2009:07:09 11:50:00
Modify Date                  : 2009:12:29 16:11:00
Page Count                   : 1
Word Count                   : 717
Char Count                   : 4088
Code Page                    : 1252
Company                      : CHARLIE
Lines                        : 34
Paragraphs                   : 9
Char Count With Spaces       : 4796
...
```

How many times has
this scam been run
(i.e., fax number was
changed)?

When did this scam
potentially begin?

When did this actor(s)
begin their campaign?

When was this particular
fax number used?

read_open_xml

- docx format
- zip archive containing XML and binaries

```
$ read_open_xml.pl US\ ORIGINAL.docx
```

```
...
```

```
This is a word document
```

```
Application Metadata
```

```
...
```

```
TitlesOfParts = CHARLIE
```

```
Company = CHARLIE
```

```
File Metadata
```

```
title = CHARLIE
```

```
creator = ALPHA
```

```
description = ALT-F11 says it's groovie!
```

```
lastModifiedBy = BRAVO
```

```
revision = 5
```

```
lastPrinted = 2009-10-25T23:02:00Z
```

```
created (xsi:type = dcterms:W3CDTF) = 2010-03-07T18:33:00Z
```

```
modified (xsi:type = dcterms:W3CDTF) = 2010-03-09T19:48:00Z
```


PDF

- “merely converting an MS Word document to PDF does not remove all metadata automatically” (NSA)
- various tools exist for both analyzing suspicious PDFs (malware) and for extracting metadata
- tools
 - pdftk, pdftk, pdfid, pdf-parser

pdftinfo

\$ pdftinfo irs\ form-1.pdf

Title: Microsoft Word - irs form-1
Author: ALPHA
Creator: PScript5.dll Version 5.2
Producer: GPL Ghostscript 8.64
CreationDate: Wed Mar 10 15:38:08 2010
ModDate: Wed Mar 10 15:38:08 2010
Tagged: no
Pages: 1
Encrypted: no
Page size: 612 x 792 pts (letter)
File size: 37973 bytes
Optimized: no
PDF version: 1.3

pdftk

\$pdftk irs\ form-1.pdf dump_data output report.txt

InfoKey: Creator

InfoValue: PScript5.dll Version 5.2

InfoKey: Title

InfoValue: Microsoft Word - irs form-1

InfoKey: Author

InfoValue: ALPHA

InfoKey: Producer

InfoValue: GPL Ghostscript 8.64

InfoKey: ModDate

InfoValue: D:20100310153808-05'00'

InfoKey: CreationDate

InfoValue: D:20100310153808-05'00'

PdfID0: d92a6bd4a756f3546384084cc68d130

PdfID1: d92a6bd4a756f3546384084cc68d130

NumberOfPages: 1

pdfid

```
$ pdfid.py irs\ letter-2.pdf
```

```
PDFiD 0.0.9 irs letter-2.pdf
```

```
PDF Header: %PDF-1.3
```

obj	31
endobj	31
stream	9
endstream	9
xref	1
trailer	1
startxref	1
/Page	1
/Encrypt	0
/ObjStm	0
/JS	0
/JavaScript	0
/AA	0
/OpenAction	0
/AcroForm	0
/JBIG2Decode	0
/RichMedia	0
/Colors > 2^24	0

pdf-parser

\$ pdf-parser.py irs\ letter-2.pdf | grep Author

```
[(1, '\n'), (2, '<<'), (2, '/Producer'), (2, '('), (3, 'GPL'), (1, ' '), (3,
  'Ghostscript'), (1, ' '), (3, '8.64'), (2, ')'), (1, '\n'), (2, '/CreationDate'), (2,
  '('), (3, "D:20100310153954-05'00'"), (2, ')'), (1, '\n'), (2, '/ModDate'), (2,
  '('), (3, "D:20100310153954-05'00'"), (2, ')'), (1, '\n'), (2, '/Title'), (2, '('),
  (3, 'Microsoft'), (1, ' '), (3, 'Word'), (1, ' '), (3, '-'), (1, ' '), (3, 'irs'), (1, ' '),
  (3, 'letter-2'), (2, ')'), (1, '\n'), (2, '/Creator'), (2, '('), (3, 'PScript5.dll'), (1, '
  '), (3, 'Version'), (1, ' '), (3, '5.2'), (2, ')'), (1, '\n'), (2, '/Author'), (2, '('), (3,
  'ALPHA'), (2, ')'), (2, '>>')]
```

/Author (ALPHA)

Images

- EXIF - Extensible Image Format
- Extraction
 - Exifviewer
 - Exifprobe
- Comparison
 - ImageMagick (PerlMagick)
 - compare

Comparison (compare)

- Metadata “creation”
 - If an artifact (DOC, PDF, scanned document) is not an image, make one
 - Word to PDF, PDF to Tiff, Tiff to JPEG
- Analyze differences
 - ImageMagick (PerlMagick) libraries
 - compare utility

FORM W-8BEN (NRA Recertification)
Request for Recertification of Foreign Status
(NOVEMBER, 2009)

W-8BEN		Certificate of Foreign Status of Beneficial Owner	
(Substitute form)		For United States Tax Withholding	
Part I Identification of Beneficial Owner			
1. Name of individual or organization that is the beneficial owner		2. Sex: <input type="checkbox"/> male <input type="checkbox"/> female	
3. Type of beneficial owner		<input type="checkbox"/> Individual <input type="checkbox"/> Corporation <input type="checkbox"/> Complex Trust	
		<input type="checkbox"/> Simple Trust <input type="checkbox"/> Grantor Trust <input type="checkbox"/> Central Bank of issue	
		<input type="checkbox"/> Government <input type="checkbox"/> International organization	
		<input type="checkbox"/> Tax-exempt organization <input type="checkbox"/> Private foundation	
4. Date of Birth			
5(a). Nationality:		5(b). Place of Birth:	
6(a). Country of permanent Residence		6(b). Passport Number:	
7. Mothers Maiden Name:			
8(a). Spouse Name:		8(b). Spouse date of Birth:	
9. Permanent resident address (street, apt. or suite no. or rural route). Do not use a P.O. box or in-care of address			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
10. Mailing address (if different from above)			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
11. Social Security Number (if any)		<input type="checkbox"/> SSN or ITIN <input type="checkbox"/> EIN	
12. Profession:		13. Day time phone/ fax Number	
14(a) Bank Name(s): *(US BANKS ONLY) *			
15. Account number(s)/Account names:			
16. Branch Address:			
17. Date Account(s) was opened:			
18. How often do you come to USA and when did you arrive last?			
19. ATTACH PHOTOCOPY OF PASSPORT FOR PROPER IDENTIFICATION			
Part II Certification of Beneficiary Owner			
Under penalties of perjury, I decided that I have examined the information on this form to the best of my knowledge and believe it is true, correct and complete. I furthermore certify under penalties of perjury that: - I am the beneficial owner (or am authorized to sign for the beneficial owner) of all the income to which this form relate. - The beneficial owner is not a U.S. person. - The income to which this form relates is not effectively connected with the conduct of a trade or business in the United States or is effectively connected but subject to tax under an income tax treaty, and - For broker transaction or barter exchanges, the beneficial owner is an exempt foreign person as defined in the instructions. Furthermore, I authorized this form to be provided to any withholding agent that has control, receipt or custody of the income of which I am the beneficial owner or withholding agent that can disburse or make payments of the income of which I am the beneficial owner. The Internal Revenue Service does not require your consent to any provisions of this document other than the Certifications required to establishing your status as a non-U.S. person and, if applicable, obtain a reduced rate of withholding.			
Sign Here			
(Signer #1) signature of beneficial owner or individual authorized to sign for beneficial owner		Date	
Sign Here			
(Signer #2) signature of beneficial owner or individual authorized to sign for beneficial owner		Date	
SEND TO FAX NO: [REDACTED]			

FORM W-8BEN (NRA Recertification)
Request for Recertification of Foreign Status
(DECEMBER, 2009)

W-8BEN		Certificate of Foreign Status of Beneficial Owner	
(Substitute form)		For United States Tax Withholding	
Part I Identification of Beneficial Owner			
1. Name of individual or organization that is the beneficial owner		2. Sex: <input type="checkbox"/> male <input type="checkbox"/> female	
3. Type of beneficial owner <input type="checkbox"/> Individual <input type="checkbox"/> Corporation <input type="checkbox"/> Complex Trust			
<input type="checkbox"/> Simple Trust <input type="checkbox"/> Grantor Trust <input type="checkbox"/> Central Bank of issue			
<input type="checkbox"/> Government <input type="checkbox"/> International organization			
<input type="checkbox"/> Tax-exempt organization <input type="checkbox"/> Private foundation			
4. Date of Birth			
5(a). Nationality:		5(b). Place of Birth:	
6(a). Country of permanent Residence		6(b). Passport Number:	
7. Mothers Maiden Name:			
8(a). Spouse Name:		8(b). Spouse date of Birth:	
9 Permanent resident address (street, apt, or suite no, or rural route). Do not use a P.O. box or In-care of address			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
10. Mailing address (if different from above)			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
11. Social Security Number (if any) <input type="checkbox"/> SSN or ITIN <input type="checkbox"/> EIN			
12. Profession:		13. Day time phone/ fax Number	
14(a) Bank Name(s): *(US BANKS ONLY) *			
15. Account number(s)/Account names:			
16. Branch Address:			
17. Date Account(s) was opened:			
18. How often do you come to USA and when did you arrive last?			
19. ATTACH PHOTOCOPY OF PASSPORT FOR PROPER IDENTIFICATION			
Part II Certification of Beneficiary Owner			
Under penalties of perjury, I decided that I have examined the information on this form to the best of my knowledge and believe it is true, correct and complete. I furthermore certify under penalties of perjury that: - I am the beneficial owner (or am authorized to sign for the beneficial owner) of all the income to which this form relate. - The beneficial owner is not a U.S. person. - The income to which this form relates is not effectively connected with the conduct of a trade or business in the United States or is effectively connected but subject to tax under an income tax treaty, and - For broker transaction or barter exchanges, the beneficial owner is an exempt foreign person as defined in the instructions. Furthermore, I authorized this form to be provided to any withholding agent that has control, receipt or custody of the income of which I am the beneficial owner or withholding agent that can disburse or make payments of the income of which I am the beneficial owner. The Internal Revenue Service does not require your consent to any provisions of this document other than the Certifications required to establishing your status as a non-US person and, if applicable, obtain a reduced rate of withholding.			
Sign Here _____ (Signer #1) signature of beneficial owner or individual authorized to sign for beneficial owner		_____ Date	
Sign Here _____ (Signer #2) signature of beneficial owner or individual authorized to sign for beneficial owner		_____ Date	
SEND TO FAX NO: _____			

XXXXXXXXXX

XXXXXXXXXX

FORM W-8BEN (NRA Recertification)
Request for Recertification of Foreign Status
(Substitute form)

W-8BEN		Certificate of Foreign Status of Beneficial Owner	
(Substitute form)		For United States Tax Withholding	
Part I Identification of Beneficial Owner			
1. Name of individual or organization that is the beneficial owner		2. Sex: <input type="checkbox"/> male <input type="checkbox"/> female	
3. Type of beneficial owner		<input type="checkbox"/> Individual <input type="checkbox"/> Corporation <input type="checkbox"/> Complex Trust	
		<input type="checkbox"/> Simple Trust <input type="checkbox"/> Grantor Trust <input type="checkbox"/> Central Bank of issue	
		<input type="checkbox"/> Government <input type="checkbox"/> International organization	
		<input type="checkbox"/> Tax-exempt organization <input type="checkbox"/> Private foundation	
4. Date of Birth:			
5(a). Nationality:		5(b). Place of Birth:	
6(a). Country of permanent Residence		6(b). Passport Number:	
7. Mothers Maiden Name:			
8(a). Spouse Name:		8(b). Spouse date of Birth:	
9. Permanent resident address (street, apt, or suite no, or rural route). Do not use a P.O. box or In-care of address			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
10. Mailing address (if different from above)			
City or town, state or province, include postal code where appropriate		Country (do not abbreviate)	
11. Social Security Number (if any)		<input type="checkbox"/> SSN or ITIN <input type="checkbox"/> EIN	
12. Profession:		13. Day time phone/ fax Number	
14(a) Bank Name(s): *(US BANKS ONLY) *			
15. Account number(s)/Account names:			
16. Branch Address:			
17. Date Account(s) was opened:			
18. How often do you come to USA and when did you arrive last?			
19. ATTACH PHOTOCOPY OF PASSPORT FOR PROPER IDENTIFICATION			
Part II		Certification of Beneficiary Owner	
Under penalties of perjury, I decided that I have examined the information on this form to the best of my knowledge and believe it is true, correct and complete.			
I furthermore certify under penalties of perjury that:			
<ul style="list-style-type: none">- I am the beneficial owner (or am authorized to sign for the beneficial owner) of all the income to which this form relate.- The beneficial owner is not a U.S. person.- The income to which this form relates is not effectively connected with the conduct of a trade or business in the United States or is effectively connected but subject to tax under an income tax treaty, and- For broker transaction or barter exchanges, the beneficial owner is an exempt foreign person as defined in the instructions.			
Furthermore, I authorized this form to be provided to any withholding agent that has control, receipt or custody of the income of which I am the beneficial owner or withholding agent that can disburse or make payments of the income of which I am the beneficial owner.			
The Internal Revenue Service does not require your consent to any provisions of this document other than the Certifications required to establishing your status as a non-U.S. person and, if applicable, obtain a reduced rate of withholding.			
Sign Here		_____	
(Signer #1) signature of beneficial owner or individual authorized to sign for beneficial owner		Date	
Sign Here		_____	
(Signer #2) signature of beneficial owner or individual authorized to sign for beneficial owner		Date	

SEND TO FAX NO: +1-()

Flash

Extraction

- F/OSS
 - flare
 - flasm
 - swftools (swfdump, swfstrings, swfextract)
- COTS
 - FileJuicer

flare

```
movie 'main.swf' {  
  // flash 8, total frames: 304, frame rate: 30 fps, 980x745 px,  
  compressed  
  
  movieClip 1  
    __Packages.tm.freshComponents.forms.formItems.FormItemsF  
    actory {  
    }  
  
  movieClip 2  
    __Packages.tm.freshComponents.forms.formItems.RadiobuttonI  
    tem {  
    }  
}
```


flasm

```
./flasm -d main.swf | head
```

```
movie 'main.swf' compressed // flash 8, total frames: 304, frame  
rate: 30 fps, 980x745 px
```

```
defineMovieClip 1 // total frames: 1  
end // of defineMovieClip 1
```

```
exportAssets  
1 as  
  '__Packages.tm.freshComponents.forms.formItems.FormItemsF  
  actory'  
end // of exportAssets
```


swftools (swfdump)

./swfdump main.swf | head

```
[HEADER]      File version: 8
[HEADER]      File is zlib compressed. Ratio: 90%
[HEADER]      File size: 4658353
[HEADER]      Frame rate: 30.000000
[HEADER]      Frame count: 304
[HEADER]      Movie width: 980.00
[HEADER]      Movie height: 745.00
[045]         4 FILEATTRIBUTES
[009]         3 SETBACKGROUNDCOLOR (ff/ff/ff)
[027]         4 DEFINESPRITE defines id 0001
```


swftools (swfstrings)

./swfstrings main.swf

Fusce laoreet leo vel sapien. Duis elementum leo ac metus. Sed ullamcorper elit eu sem. Proin vitae lorem. Nam eget enim ut erat varius egestas. leo, vestibulum nec, vestibulum id, nonummy. Sed mauris. Proin enim. Lorem ipsum dolor sit amet adipiscing elit.

swftools (swfextract)

`./swfextract main.swf -i`

Objects in file main.swf:

`[-i]` 95 Shapes: ID(s) 61, ... 402

`[-i]` 137 MovieClips: ID(s) 1-54, ... 404

`[-j]` 64 JPEGs: ID(s) 60, ... 395

`[-p]` 7 PNGs: ID(s) 77, ... 401

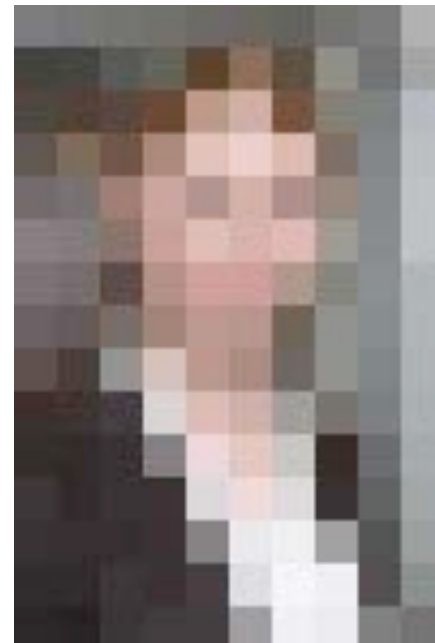
`[-s]` 8 Sounds: ID(s) 59, ... 405

`[-F]` 10 Fonts: ID(s) 55, ... 253

`[-f]` 1 Frame: ID(s) 0

`[-m]` 1 MP3 Soundstream

**`./swfextract main.swf -j 92 -o
test.swf`**



Visualization

Visualization

- visual information seeking mantra (VISM)
 - overview, zoom & filter, details of demand
- analysis examples
 - file manipulation times (gnuplot)
 - levenshtein distance (afterglow)
 - revision number (gnuplot/afterglow)

gnuplot

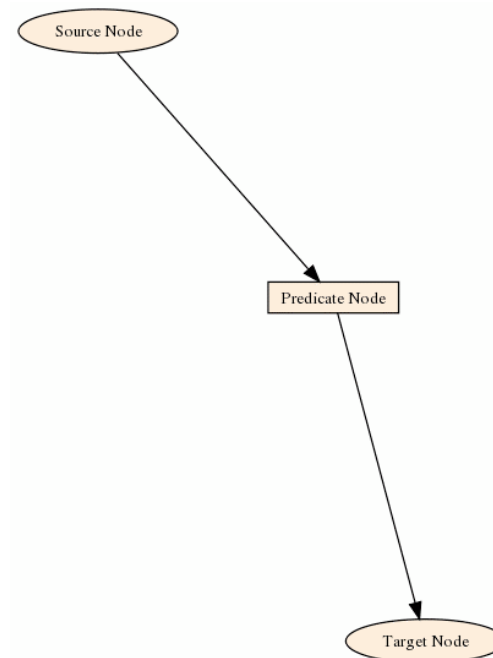
- open source graphing tool
- ability to graph multiple datasets on same graph, in 2D or 3D
- can plot large datasets easily
- easily scripted (python, perl)

afterglow

- open source software
- latest version 1.6
- creates (semantic, relationship, event) graphs, network maps, link maps
- capabilities
 - node filtering based on node name, frequency or occurrence, and fan out
 - coloring of nodes and edges
 - sizing and assigning a shape to nodes
 - aggregation of nodes

afterglow syntax

```
cat file.csv | perl afterglow.pl | neato -Tgif -o file.gif
```



AfterGlow 1.5.9

What would you rather look at?

00:41:14.900160 IP 192.168.1.72 > 8.8.8.8: ICMP
echo request, id 55251, seq 0, length 64
00:41:14.952747 IP 8.8.8.8 > 192.168.1.72: ICMP
echo reply, id 55251, seq 0, length 64
00:41:15.900238 IP 192.168.1.72 > 8.8.8.8: ICMP
echo request, id 55251, seq 1, length 64
00:41:15.952395 IP 8.8.8.8 > 192.168.1.72: ICMP
echo reply, id 55251, seq 1, length 64
00:41:16.900307 IP 192.168.1.72 > 8.8.8.8: ICMP
echo request, id 55251, seq 2, length 64
00:41:16.952026 IP 8.8.8.8 > 192.168.1.72: ICMP
echo reply, id 55251, seq 2, length 64
00:41:17.900375 IP 192.168.1.72 > 8.8.8.8: ICMP
echo request, id 55251, seq 3, length 64
00:41:17.952680 IP 8.8.8.8 > 192.168.1.72: ICMP
echo reply, id 55251, seq 3, length 64
00:41:18.900457 IP 192.168.1.72 > 8.8.8.8: ICMP
echo request, id 55251, seq 4, length 64
00:41:18.952355 IP 8.8.8.8 > 192.168.1.72: ICMP
echo reply, id 55251, seq 4, length 64
00:41:19.900540 IP 192.168.1.72 > 8.8.8.8: ICMP
echo request, id 55251, seq 5, length 64



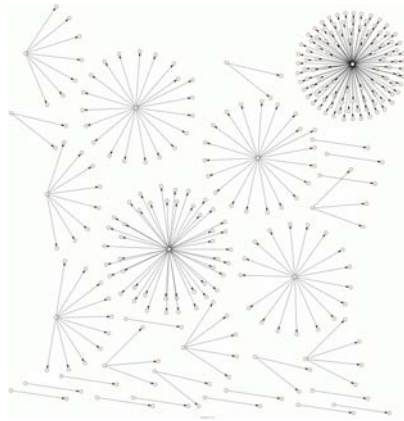
AfterGlow 1.5.9

afterglow cmd line options

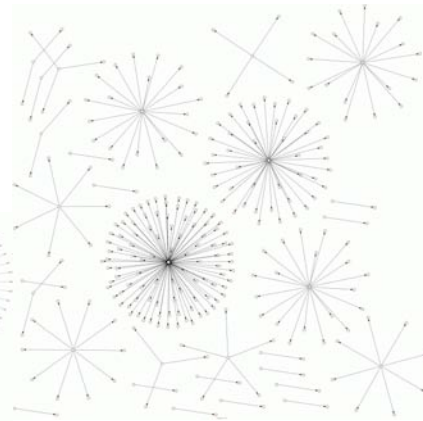
- “-a” - opsec
- “-d” - print node count
- “-t” - two-node mode
- “-f” - source fan out threshold
- “-e” - change edge length
- “-n” - suppress nodes (readability)

afterglow output options

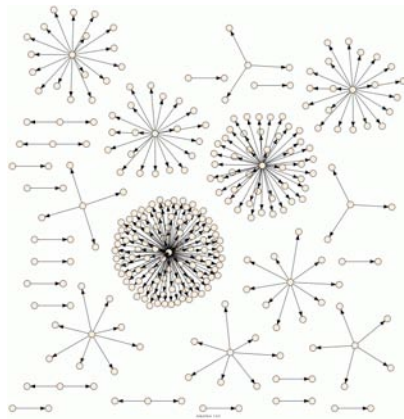
fdp



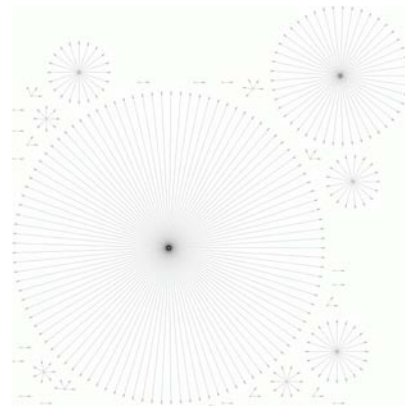
neato



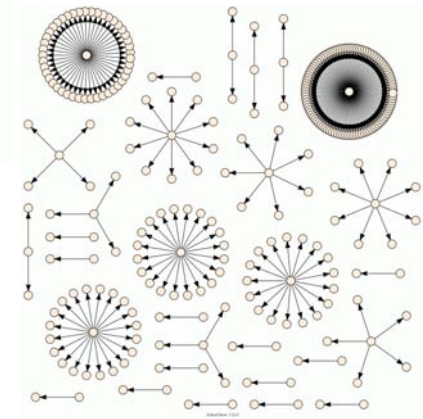
sfdp

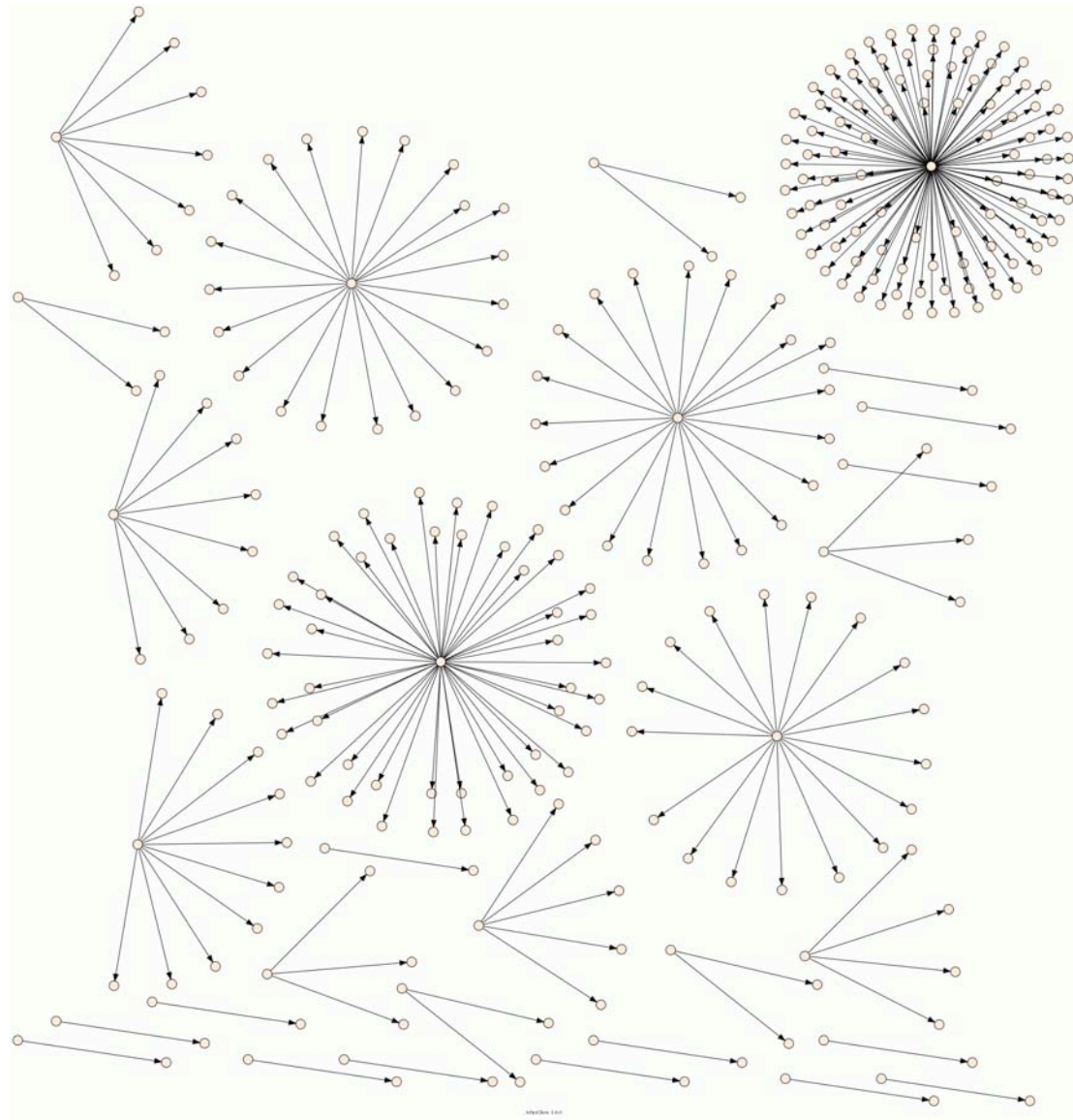


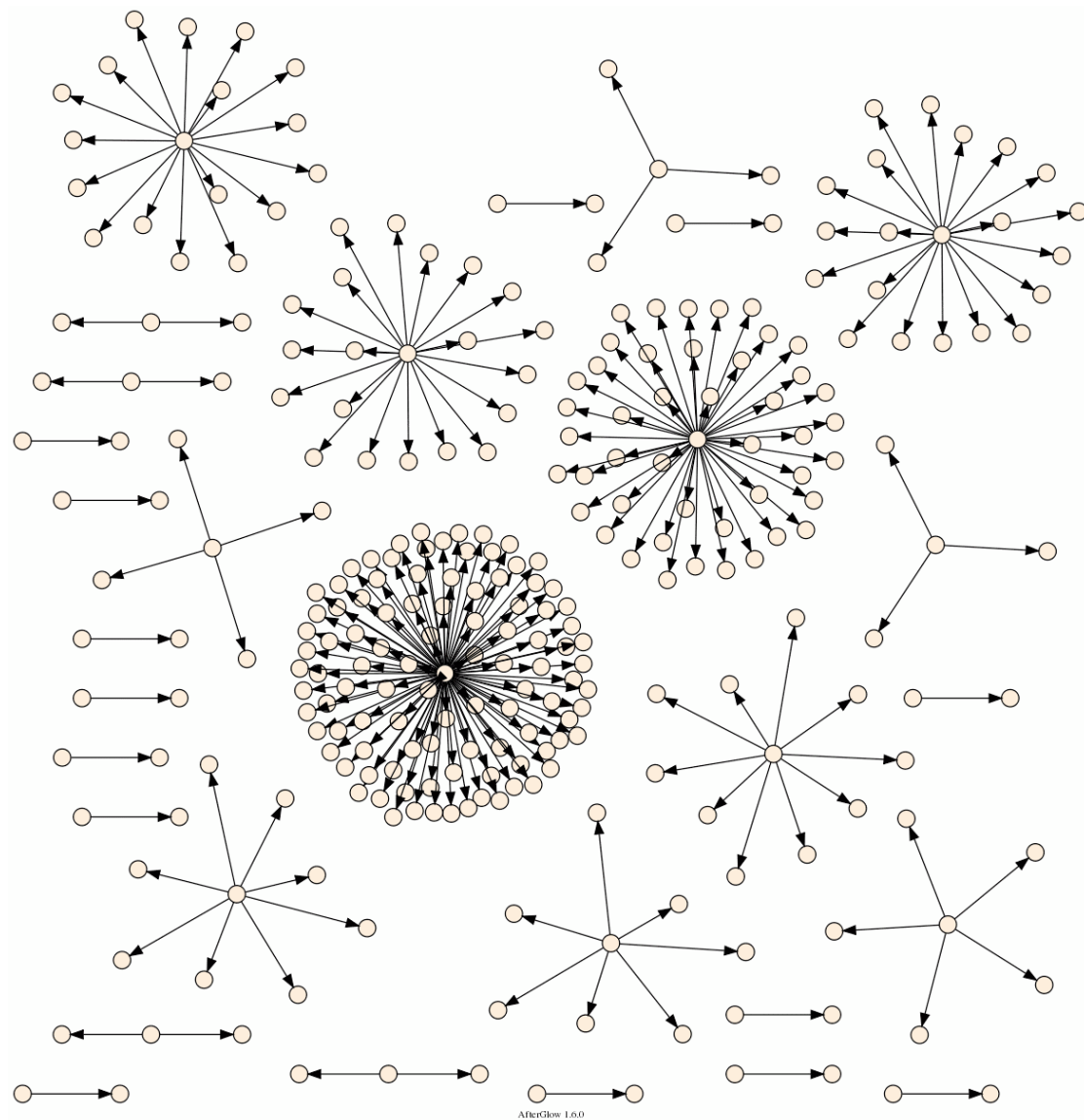
circo



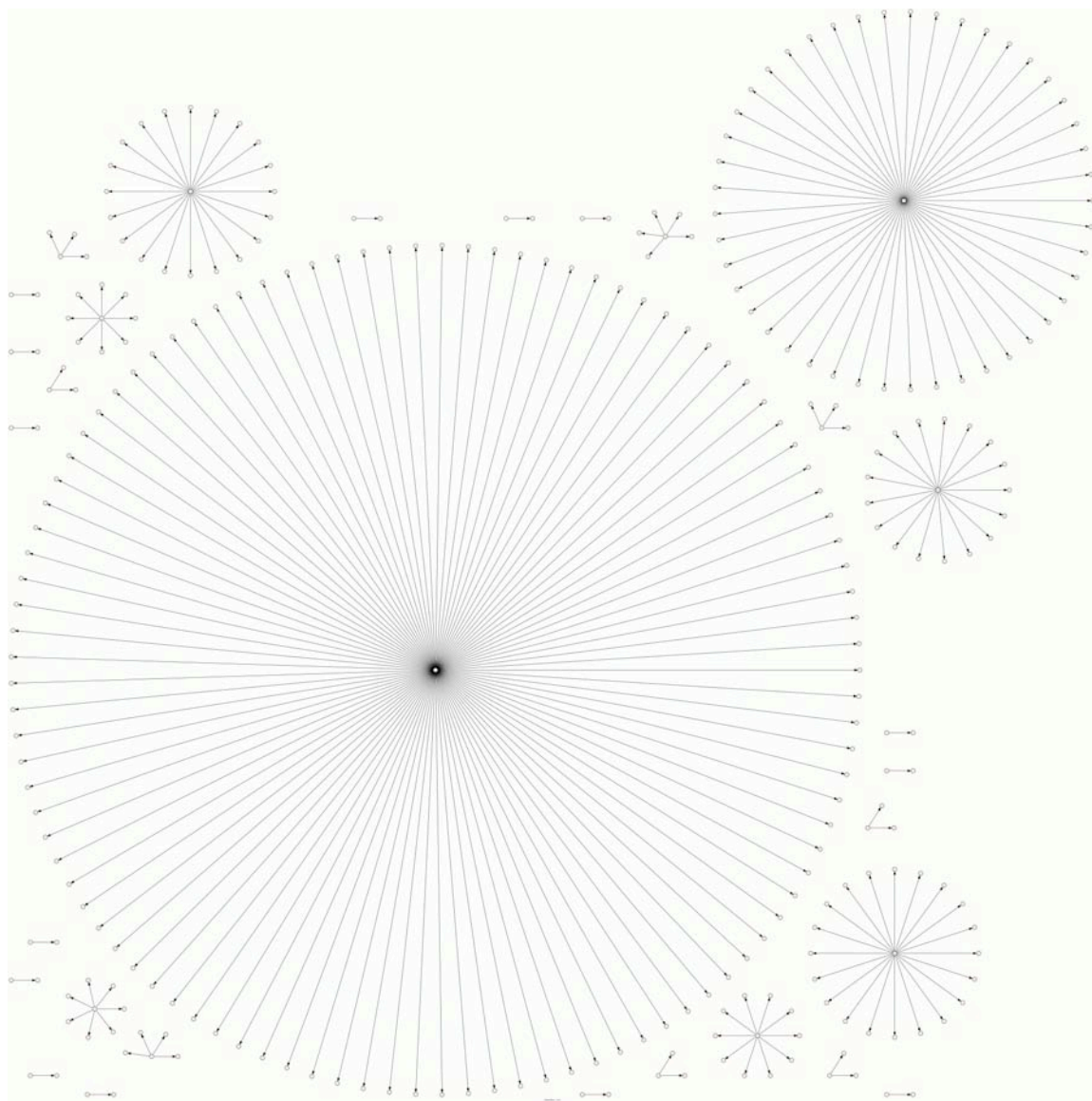
twopi

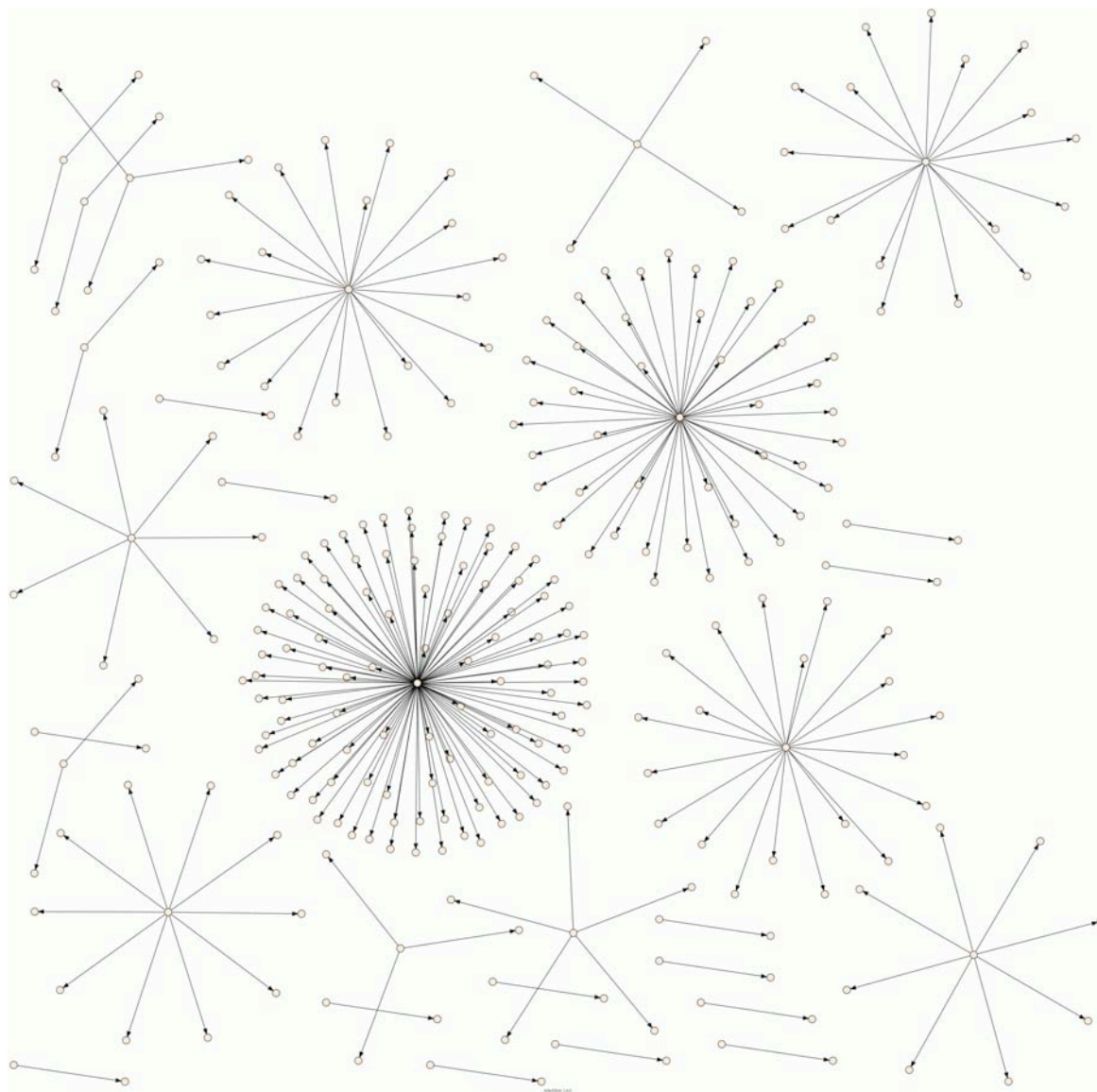


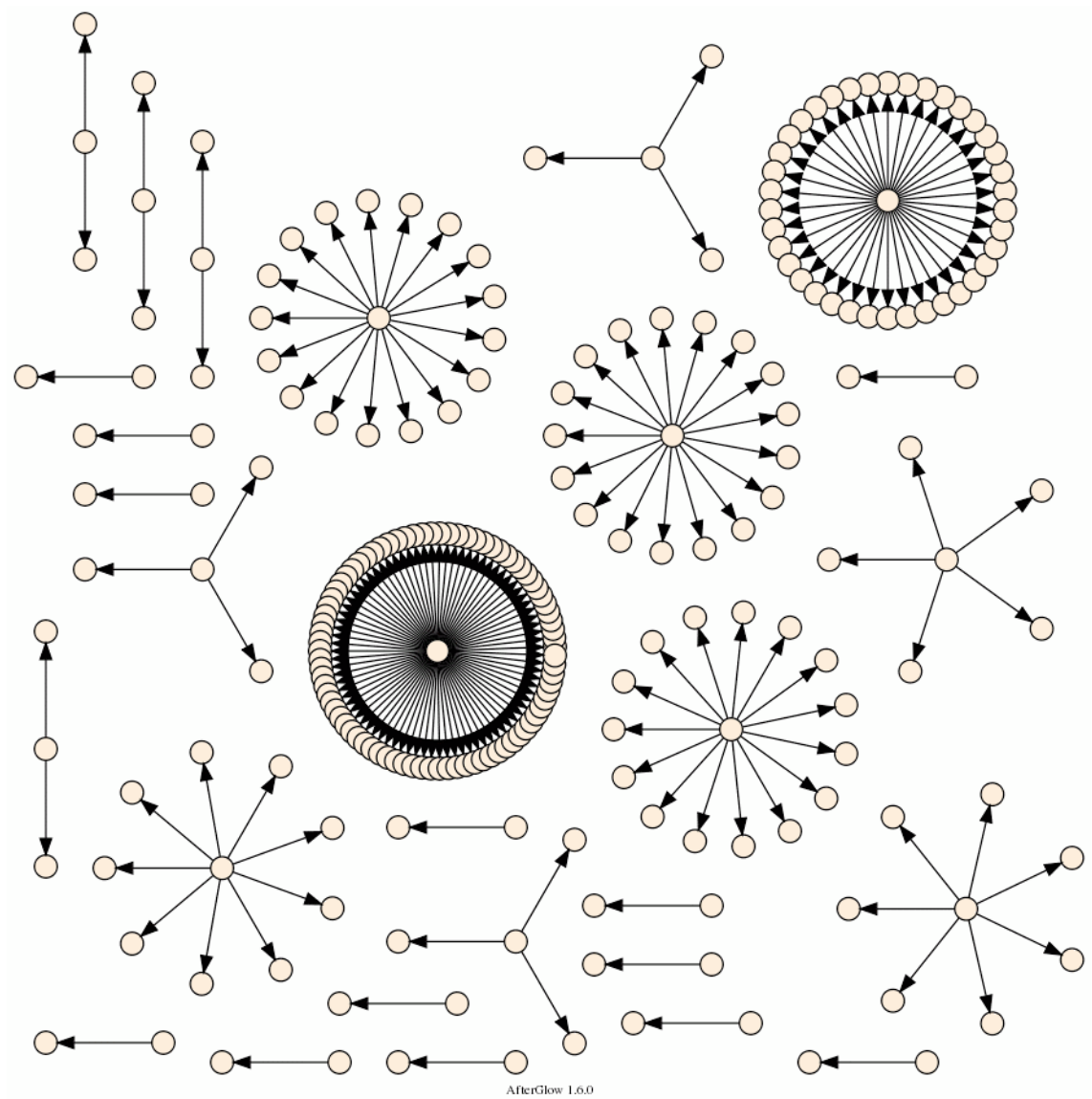




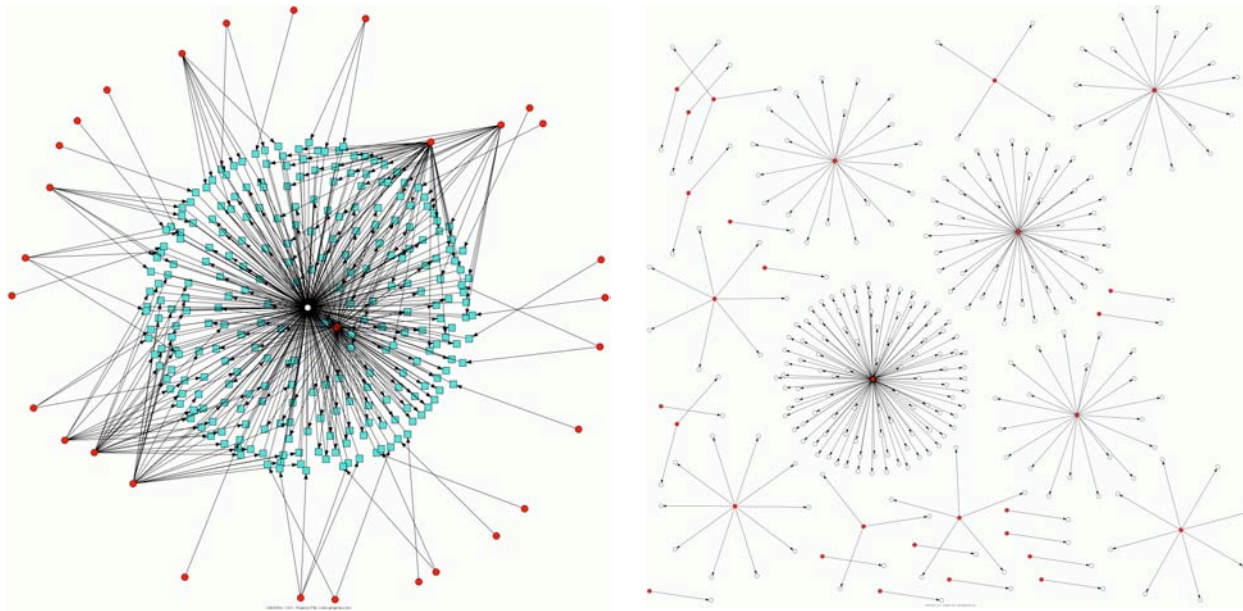
AfterGlow 1.6.0







two-node (-t) mode

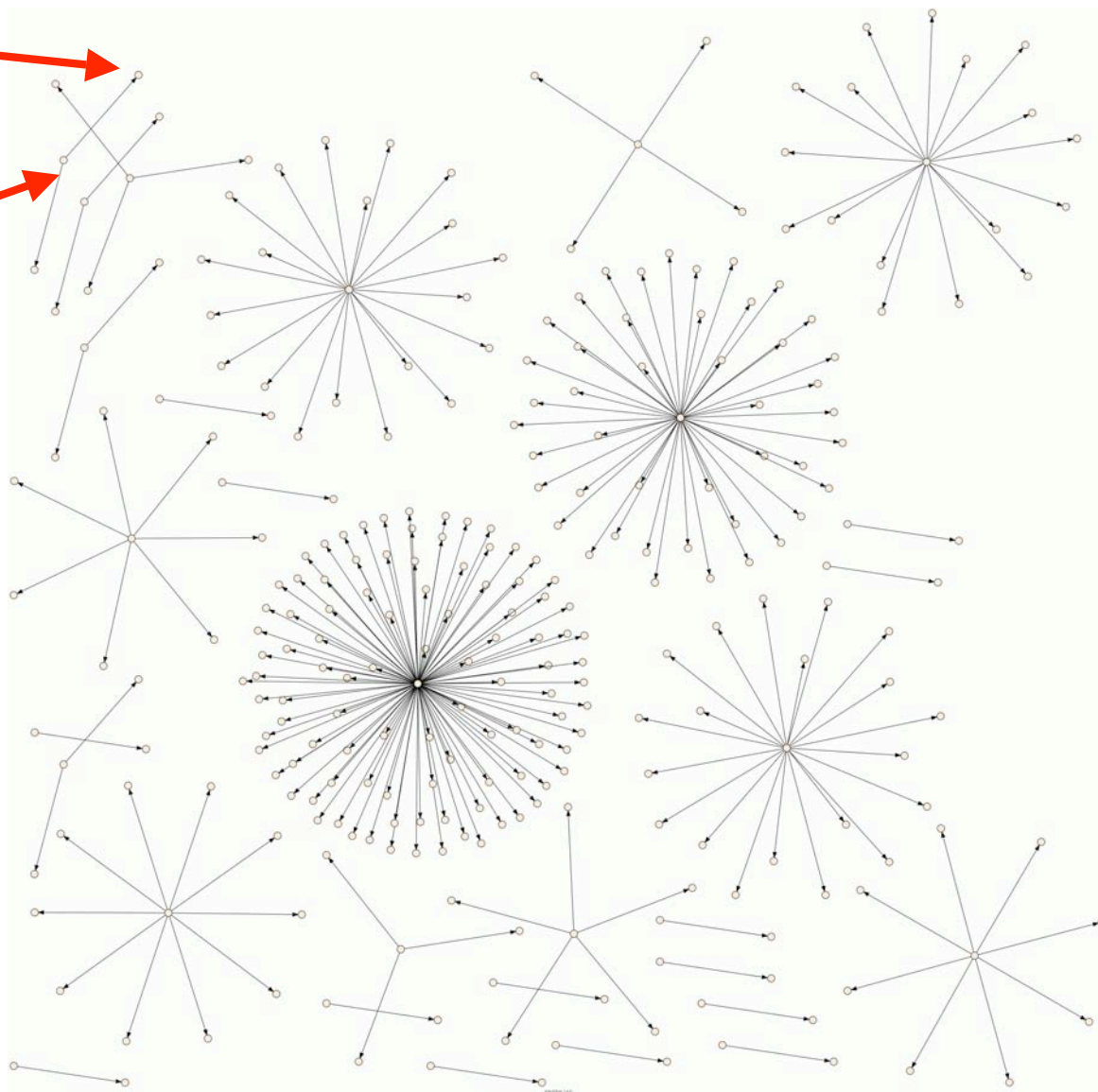


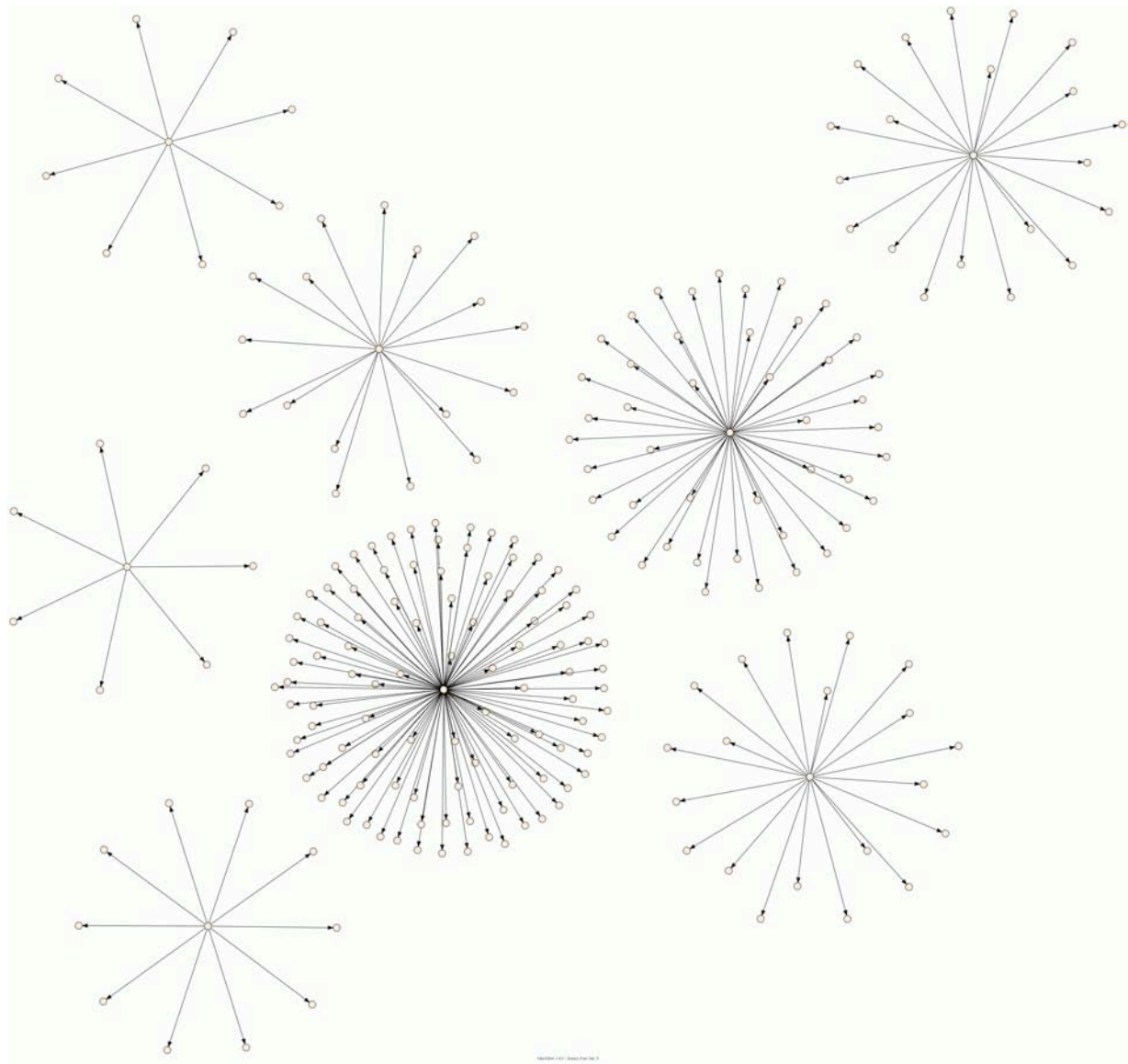
- Default is three node (source, event, target)
- “-t” skips event (source, target)

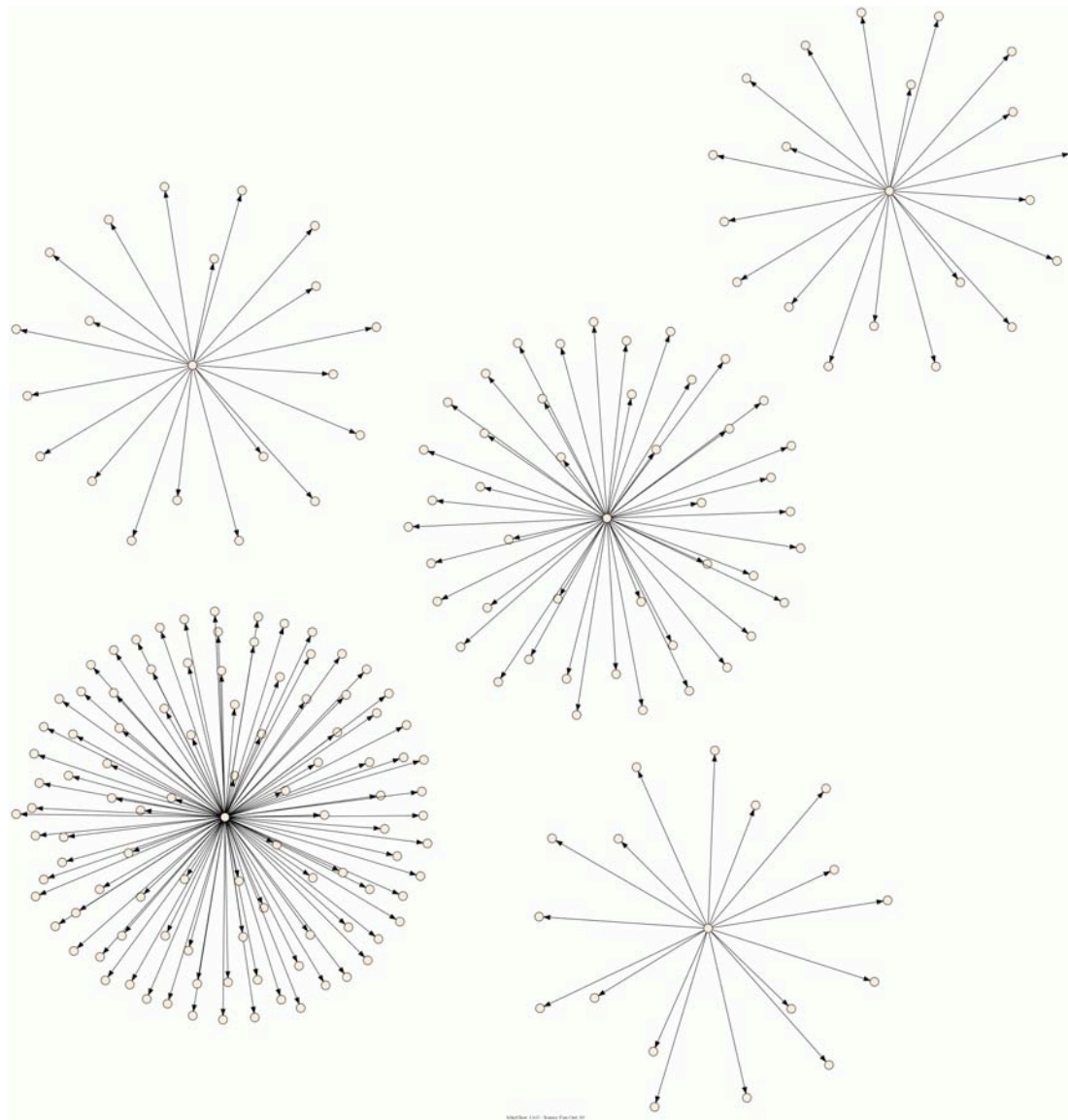
filter by source

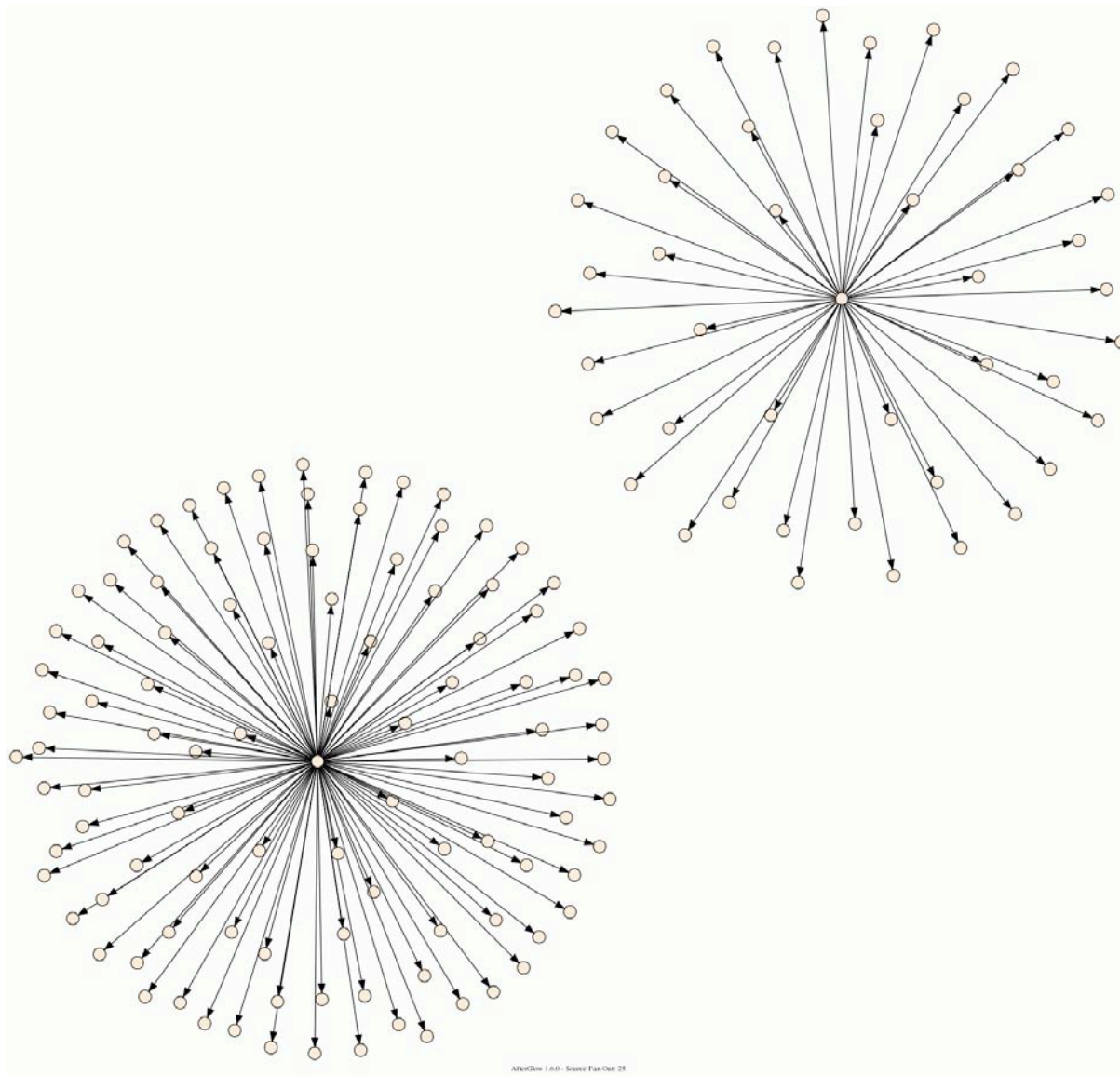
Numbers

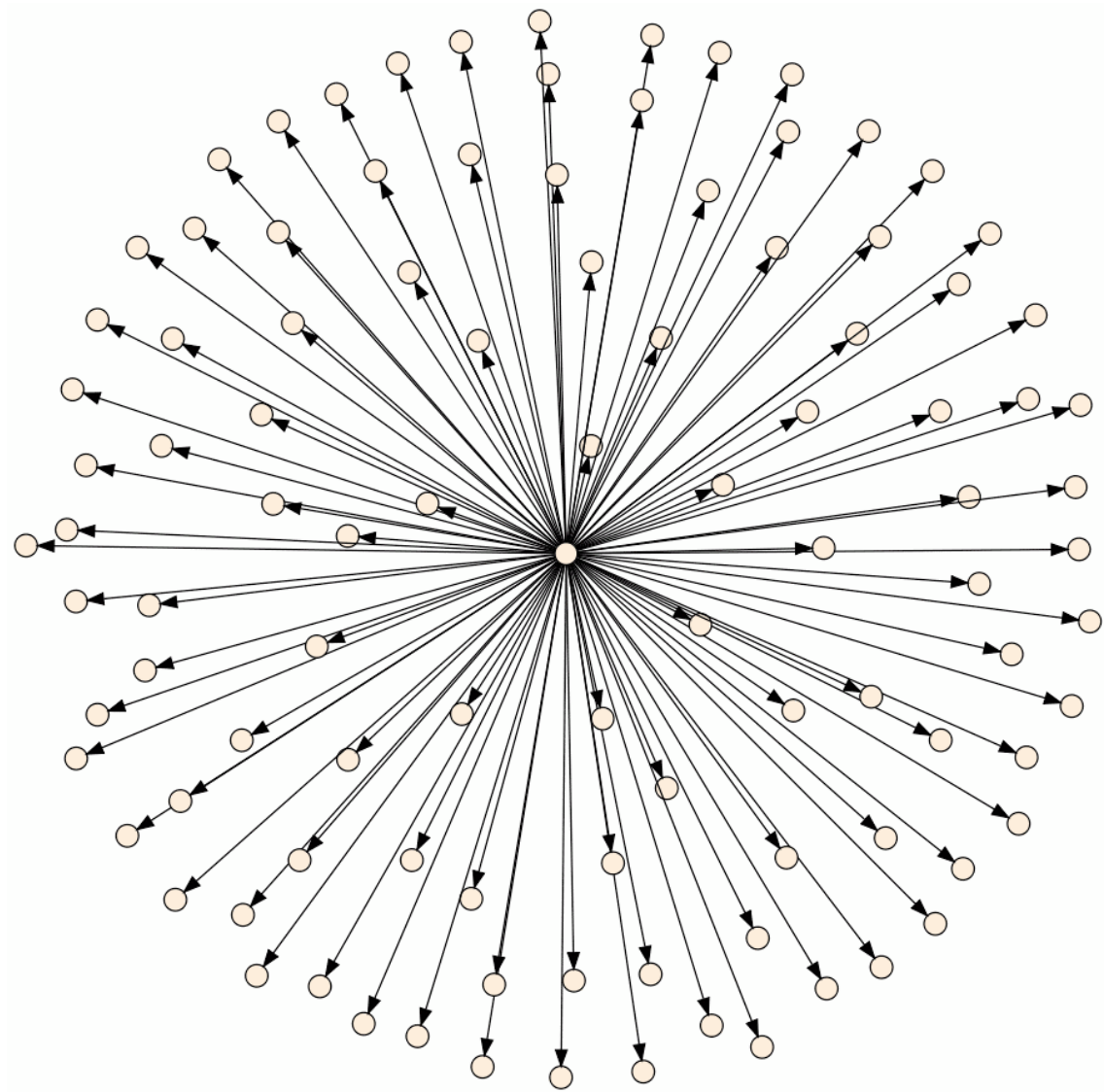
Telcos





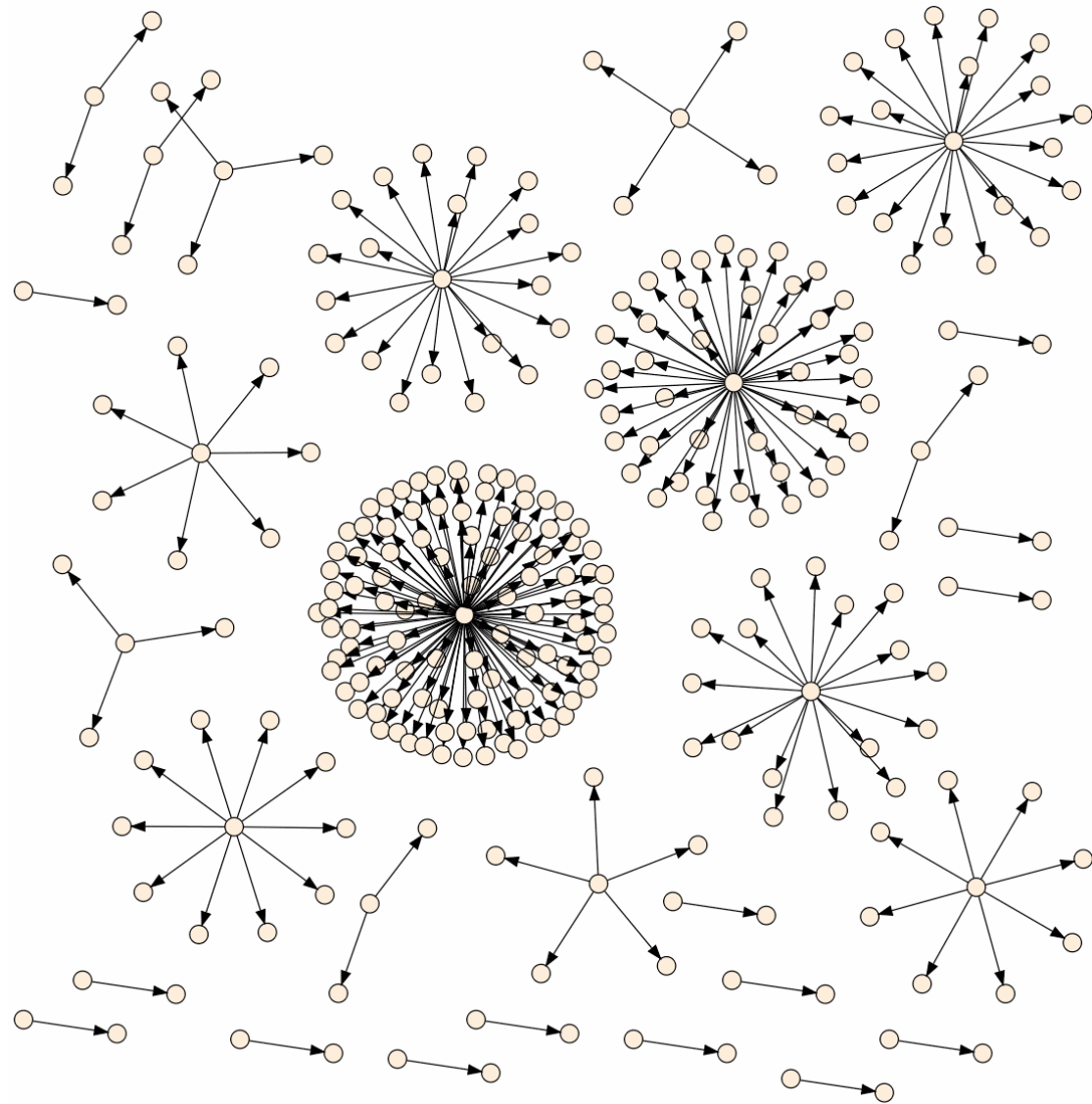


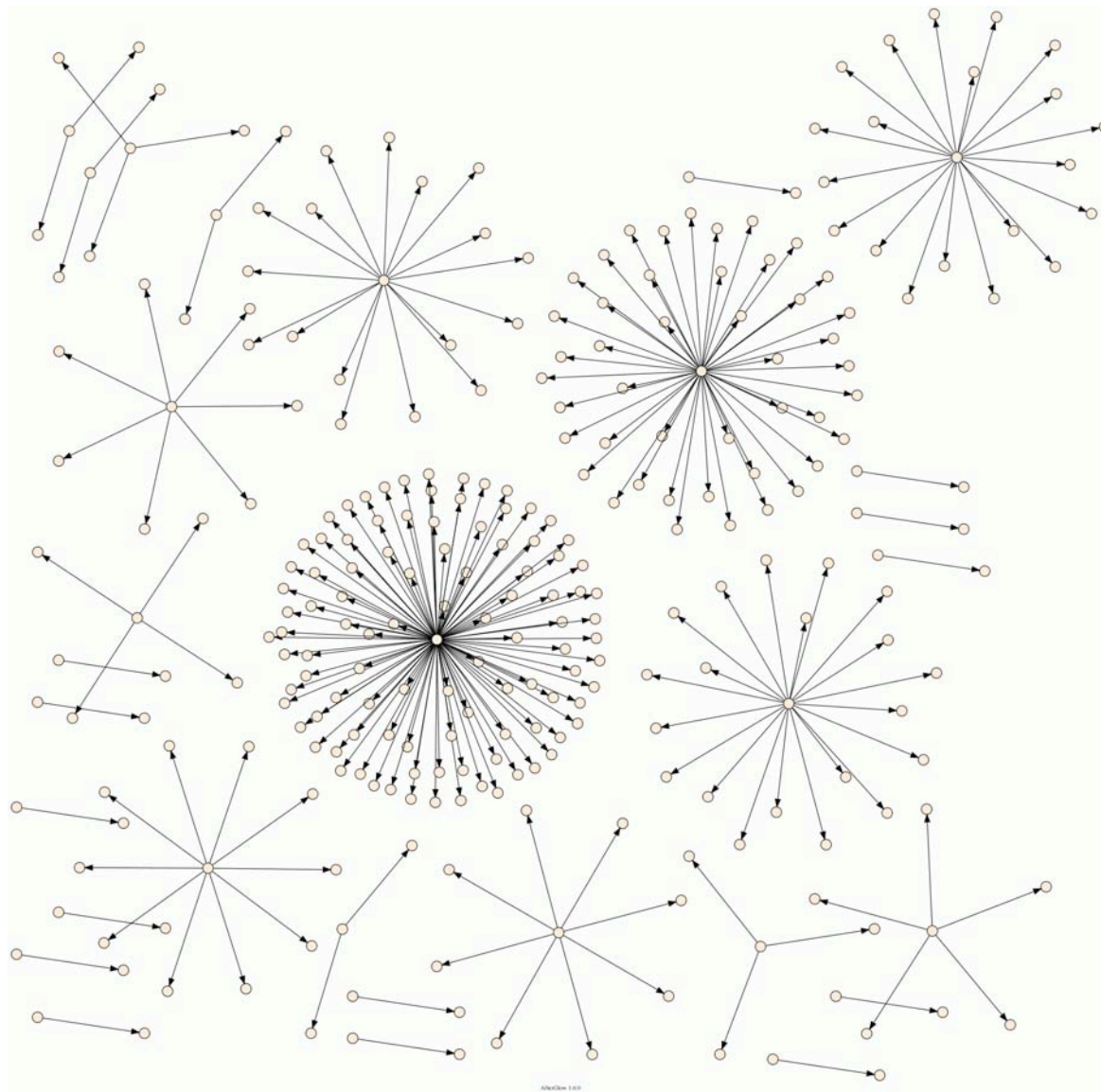


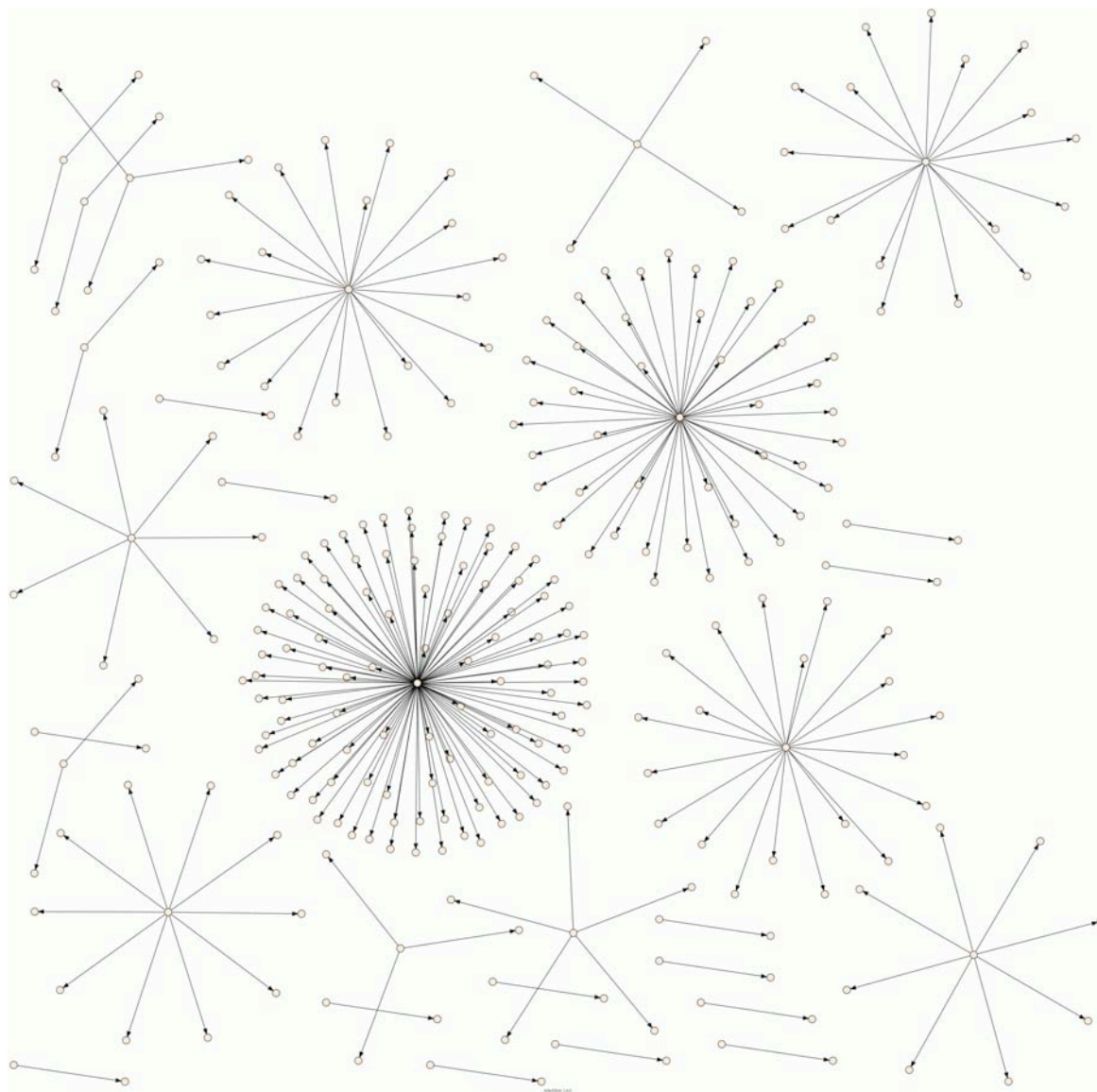


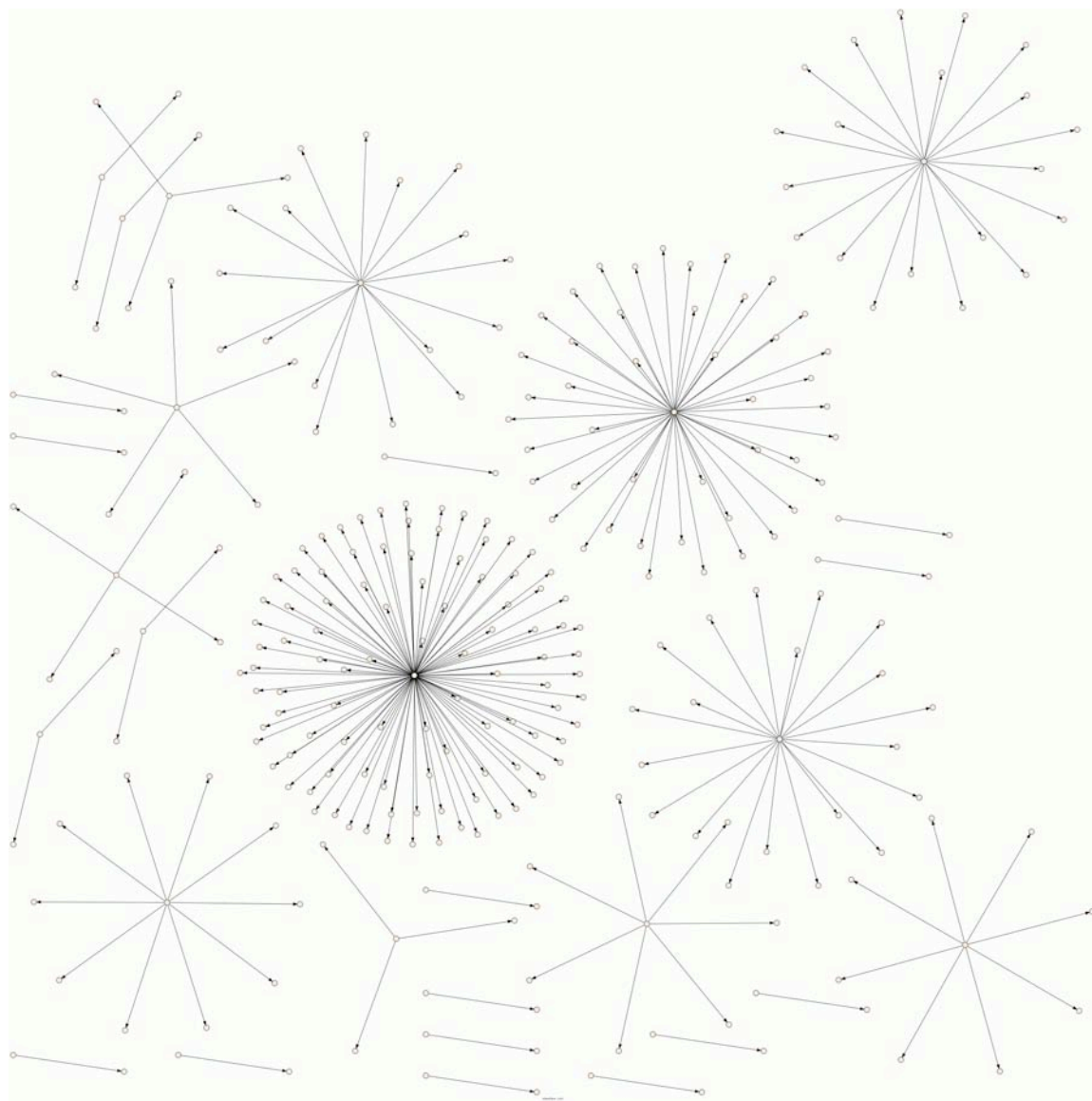
AfterGlow 1.6.0 - Source Fan Out: 50

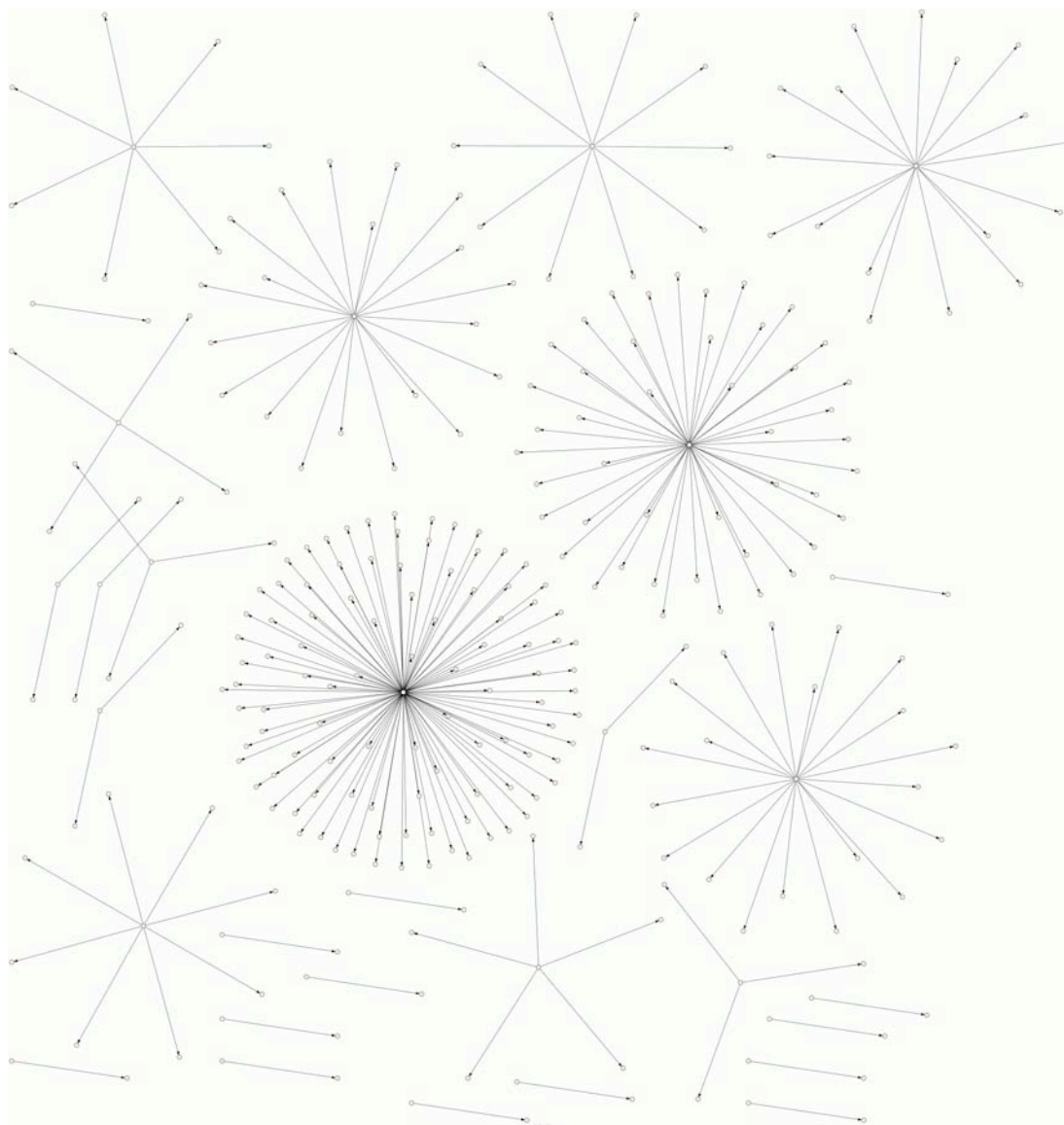
change edge length ...









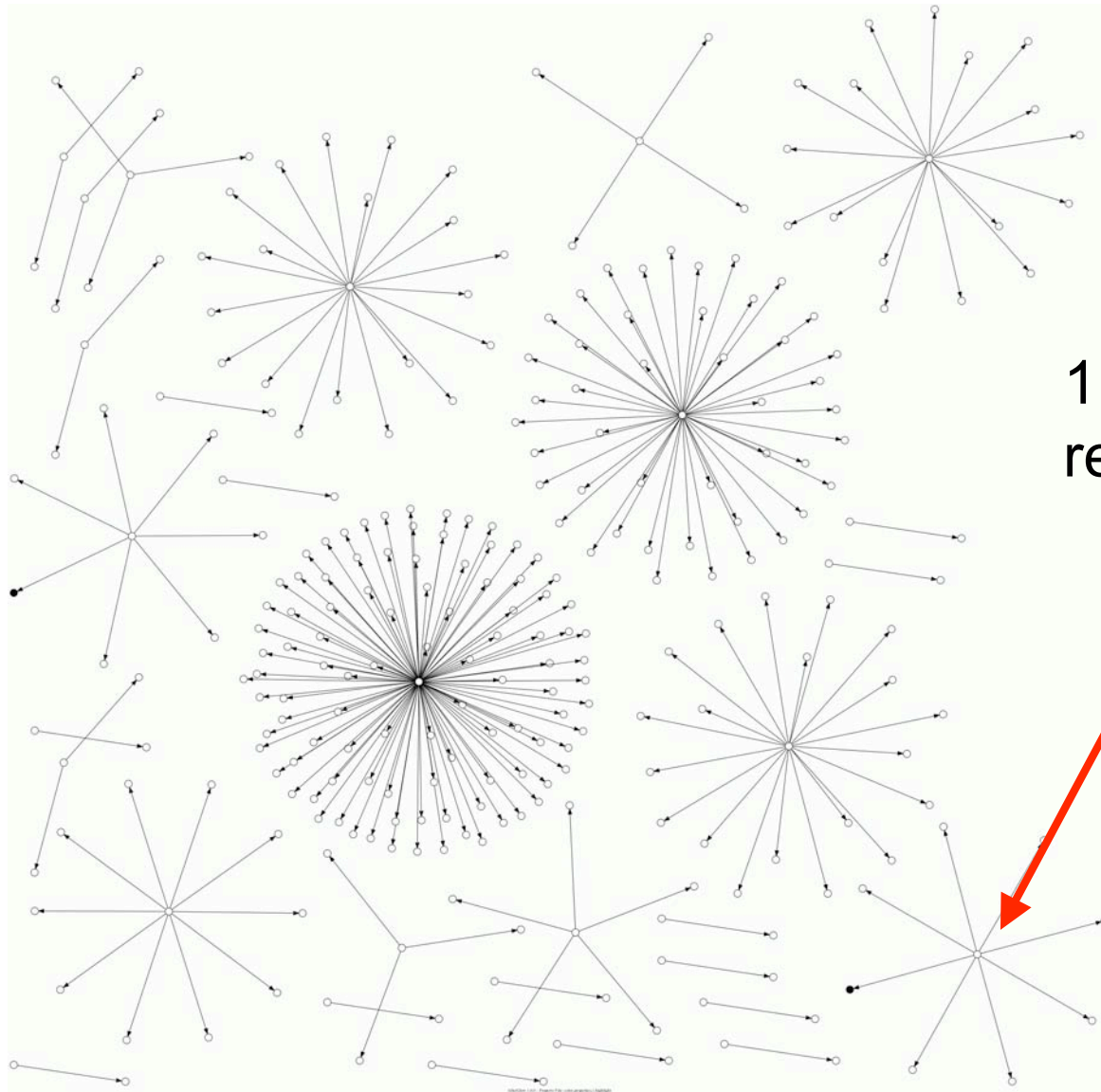


color.properties

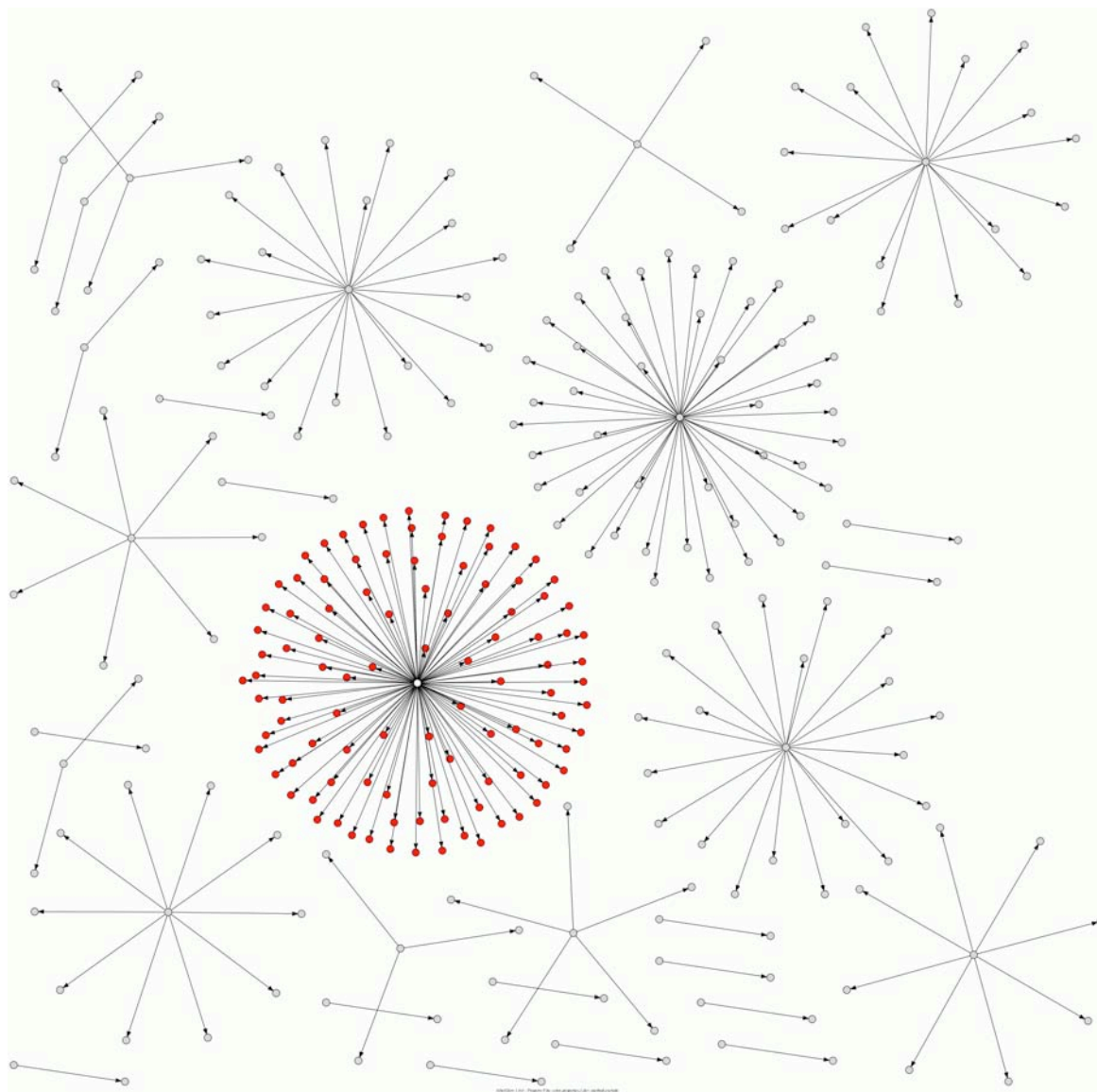
color.properties

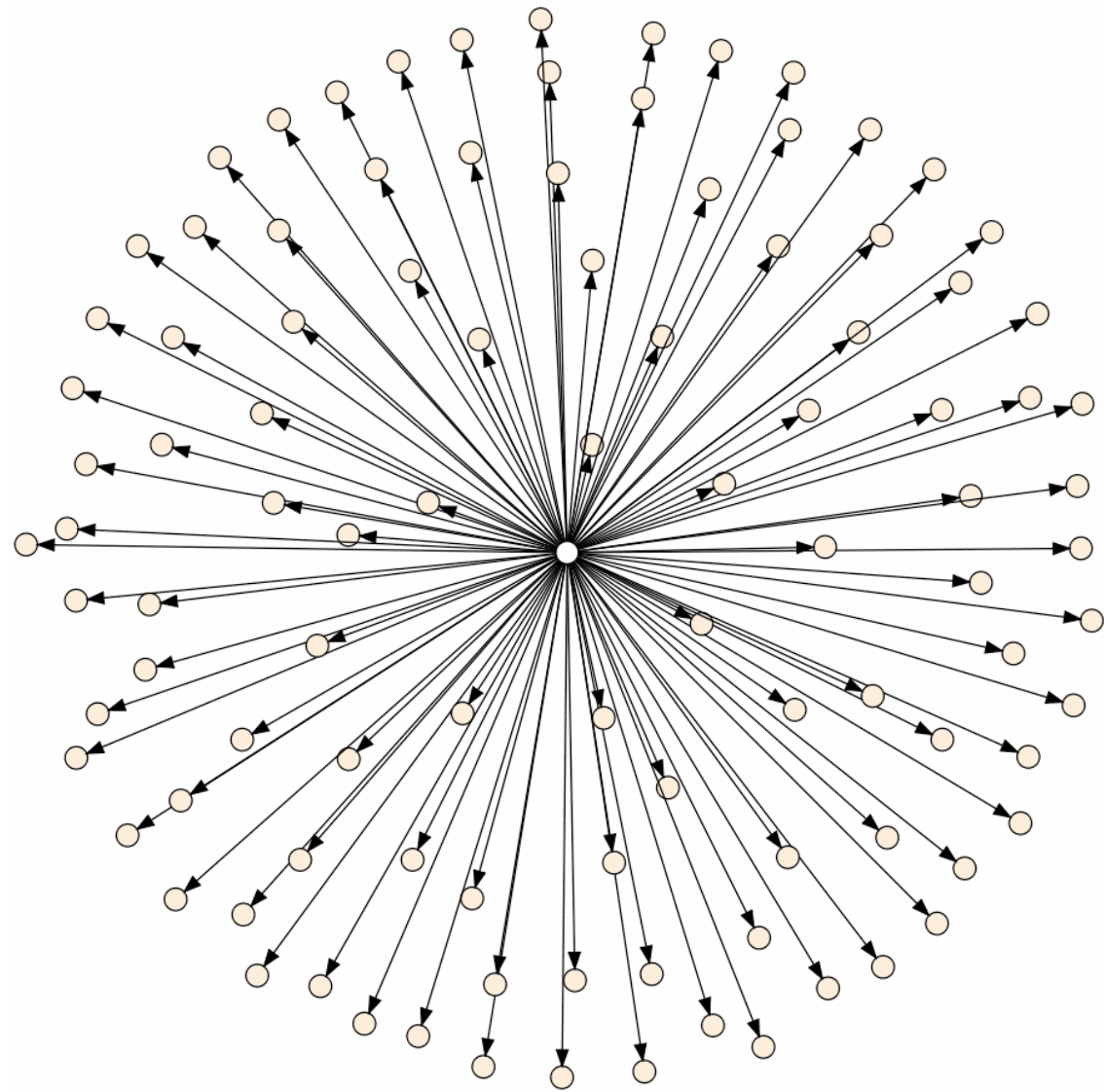
- afterglow configuration file
- Reads like firewall rules (“first match wins”)
- Adjust various aspects of the graph:
 - Color
 - Highlight specific nodes
 - Grey-out nodes
 - Isolate particular nodes
 - Remove nodes
 - Size/Shape
 - Variables

color

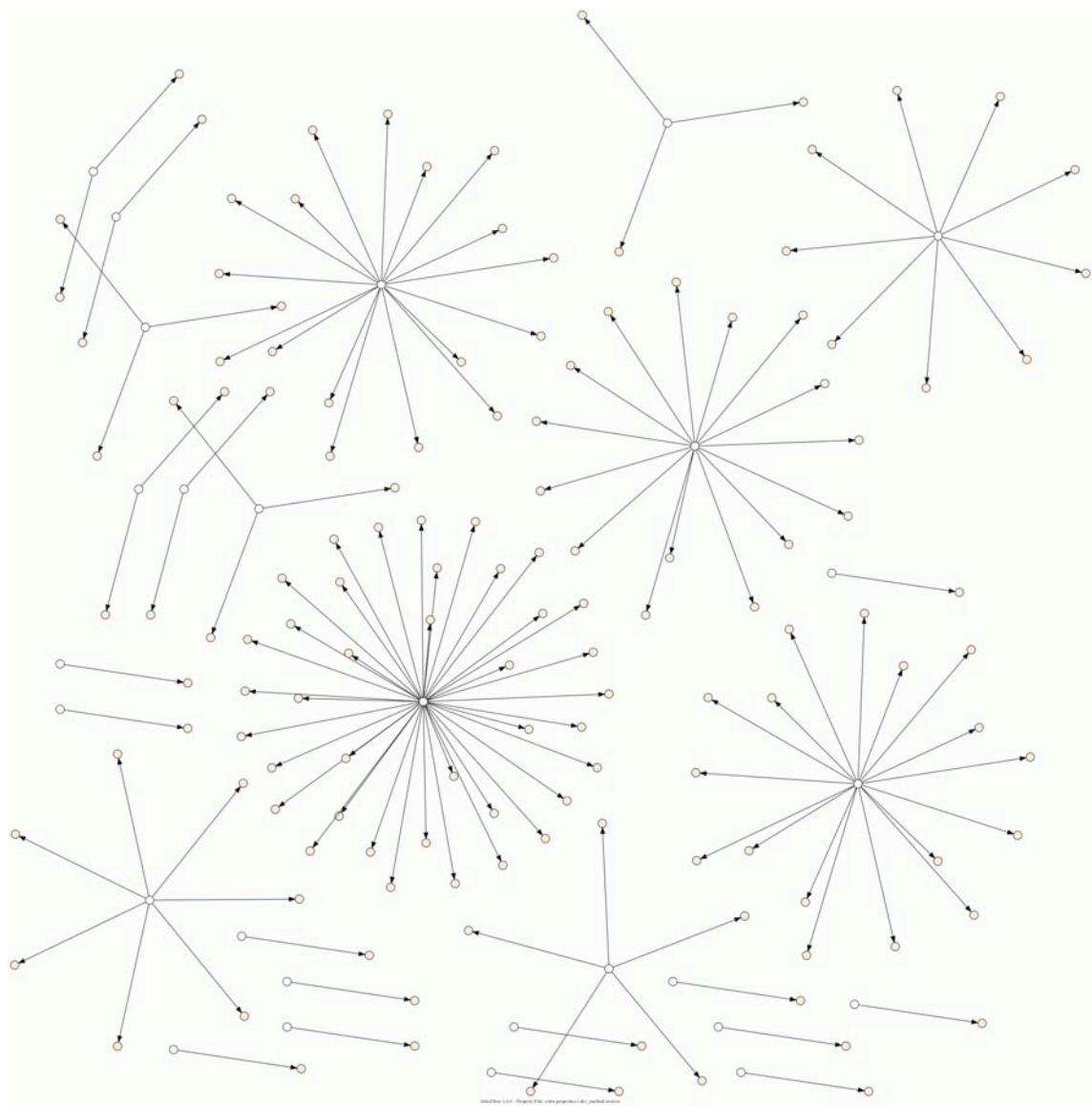


1 telco, 2 #s
re-activated





AfterGlow 1.6.0 - Property File: color.properties.1.dev_method.isolate

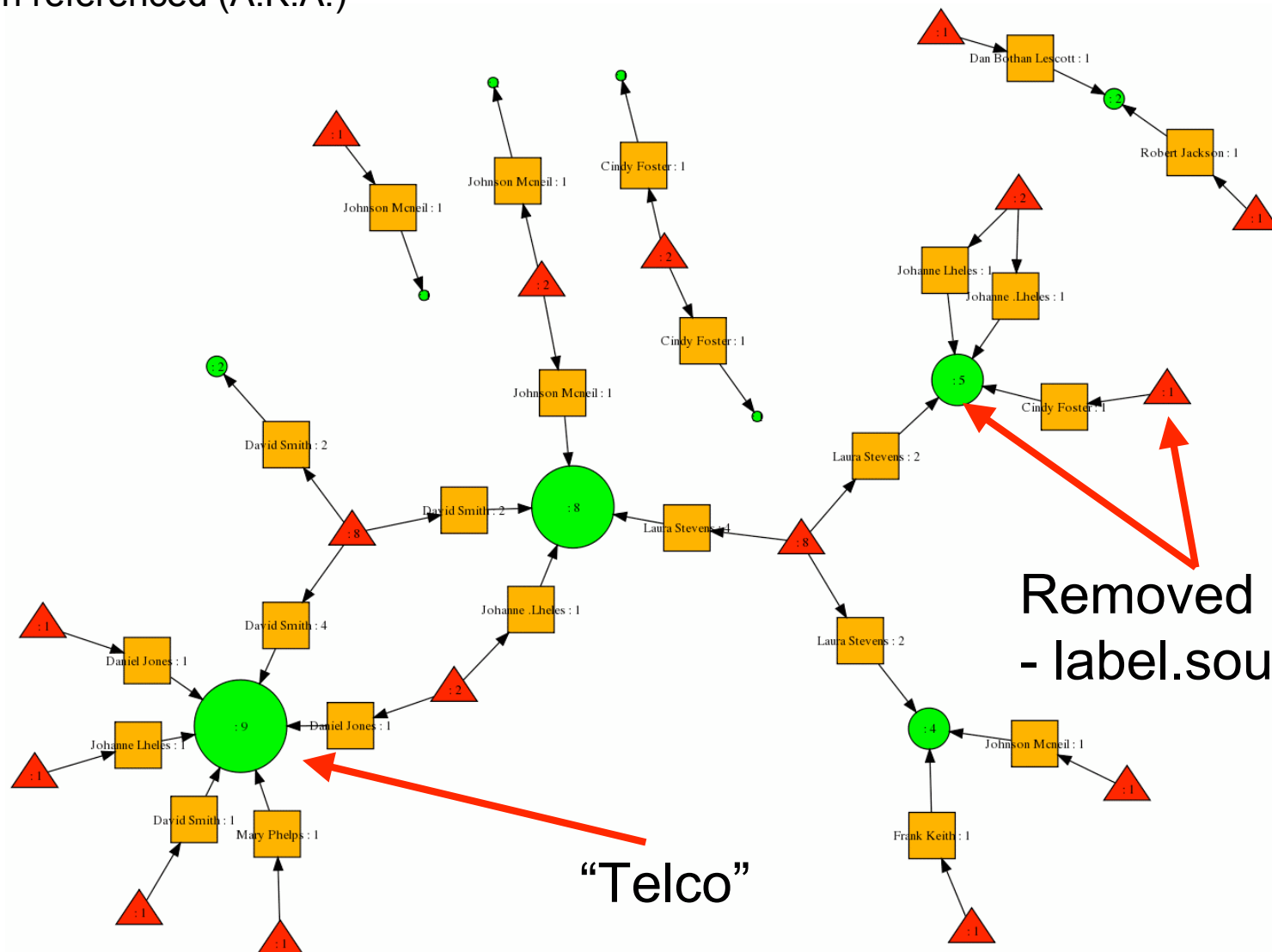


size/shape

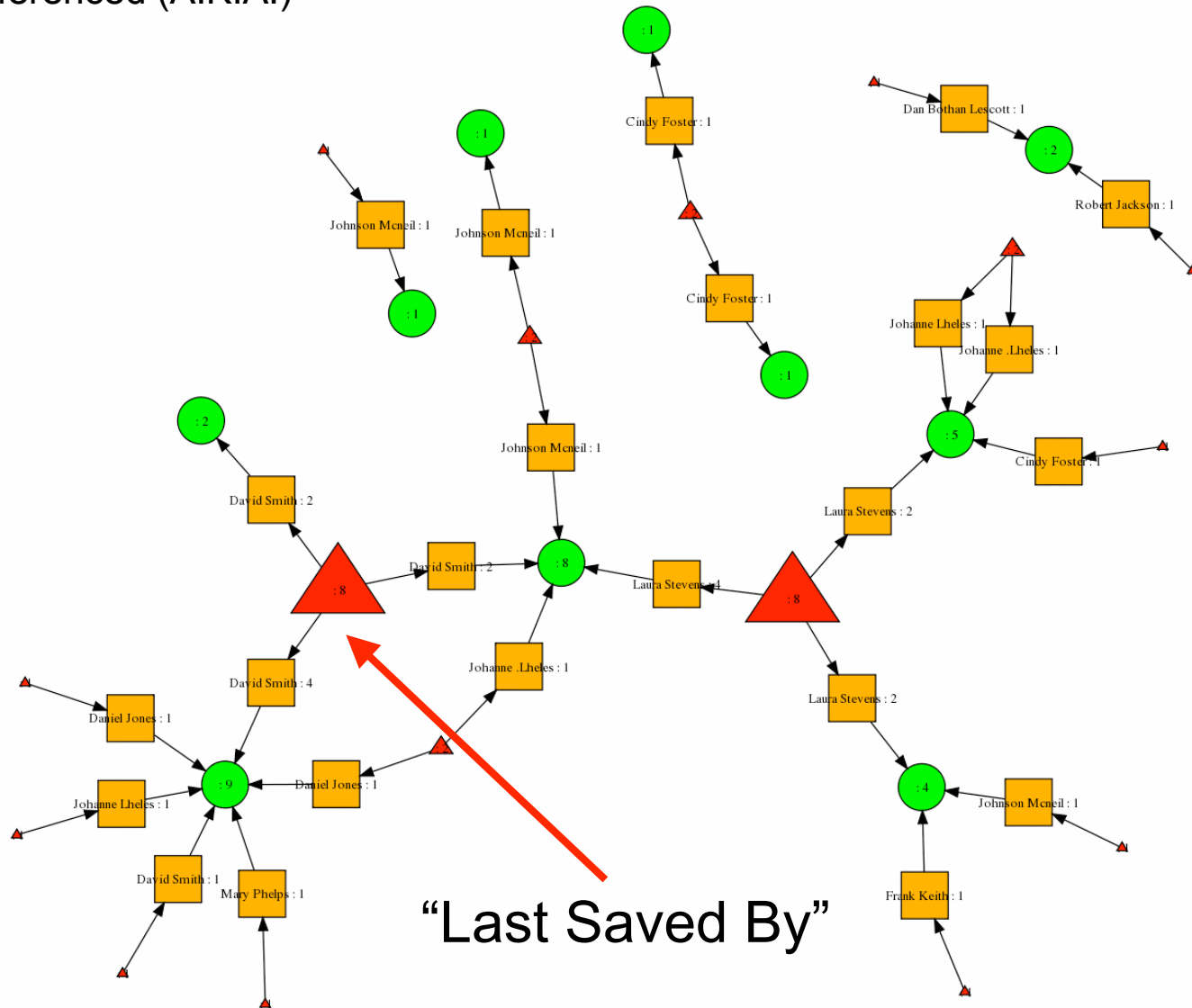
size/shape

- Helps highlight areas of interest
- Size determined by # connections
 - Last Saved By (Source) [red]
 - Person Referenced (Event) [orange]
 - Telco (Target) [green]

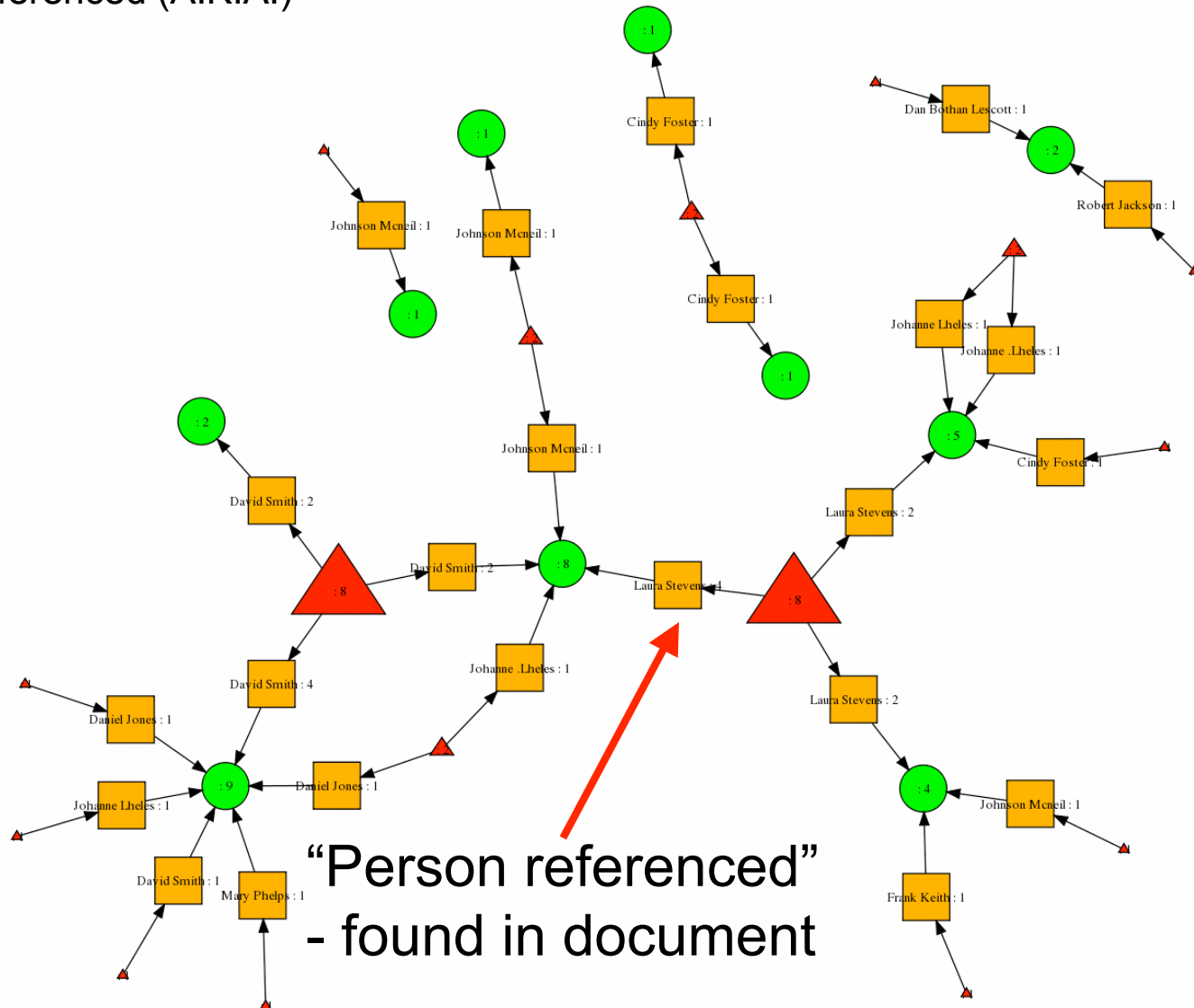
- ▲ Last Saved By
- Person referenced (A.K.A.)
- Telco



- ▲ Last Saved By
- Person referenced (A.K.A.)
- Telco



- ▲ Last Saved By
- Person referenced (A.K.A.)
- Telco

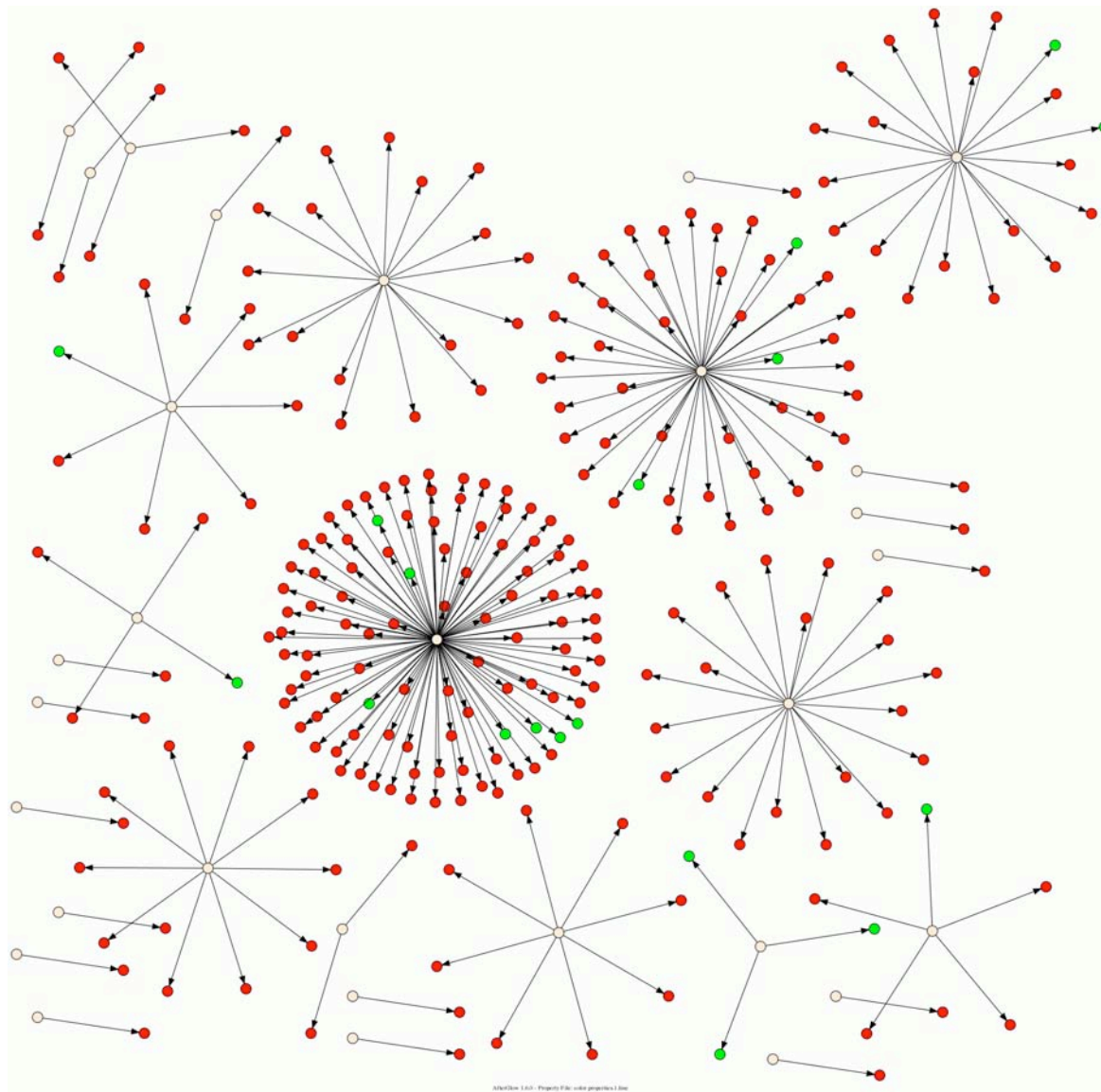


variables

- Built-in support for arrays (or lists)
- Examples
 - Data vs Voice
 - Line type
 - IRS vs Treasury
 - Brand
 - Delivery method and scam type by telco
 - Who, how, and what did they send

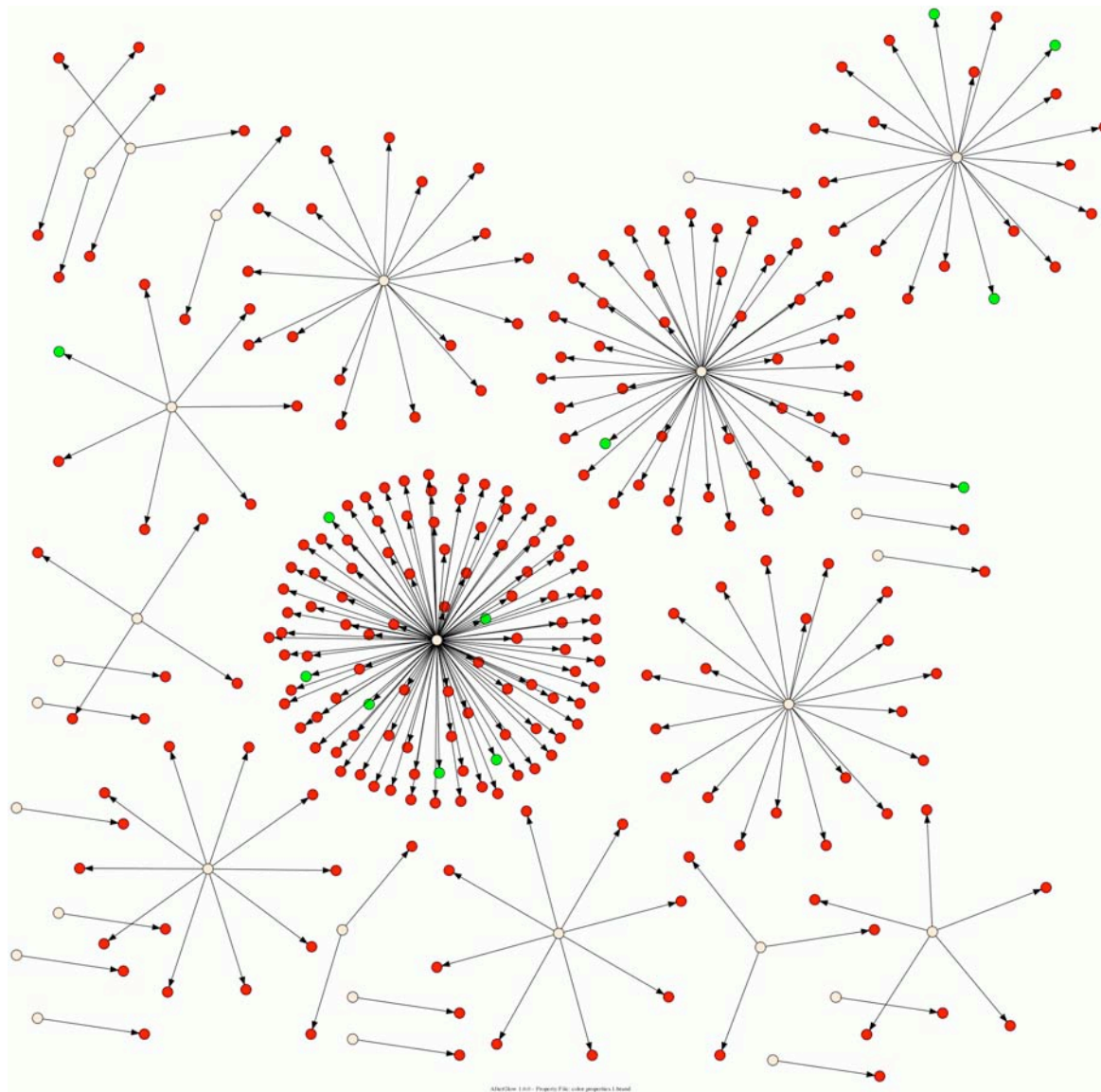
Data vs. Voice

“line type”



IRS vs. Treasury

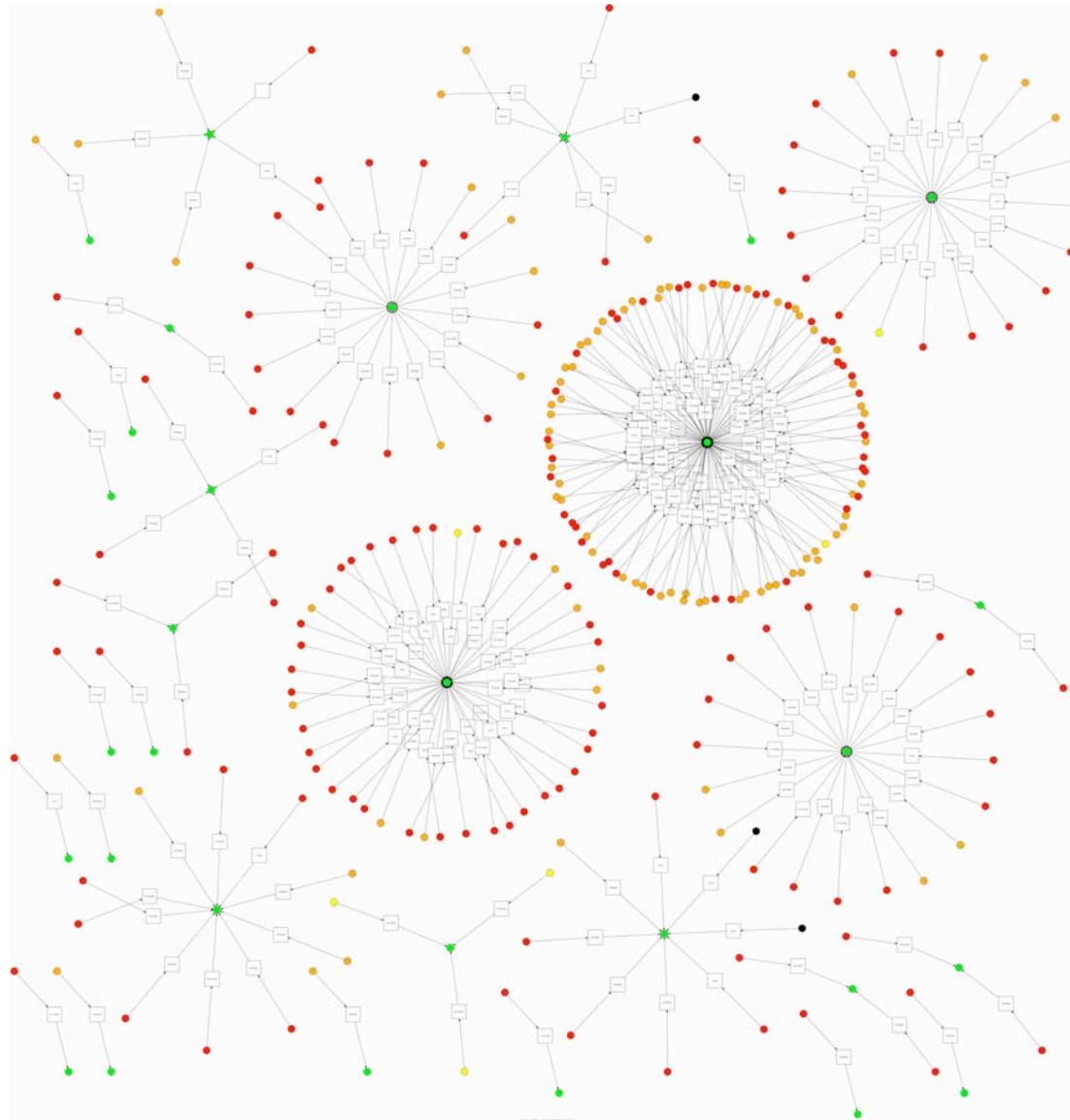
“brand”



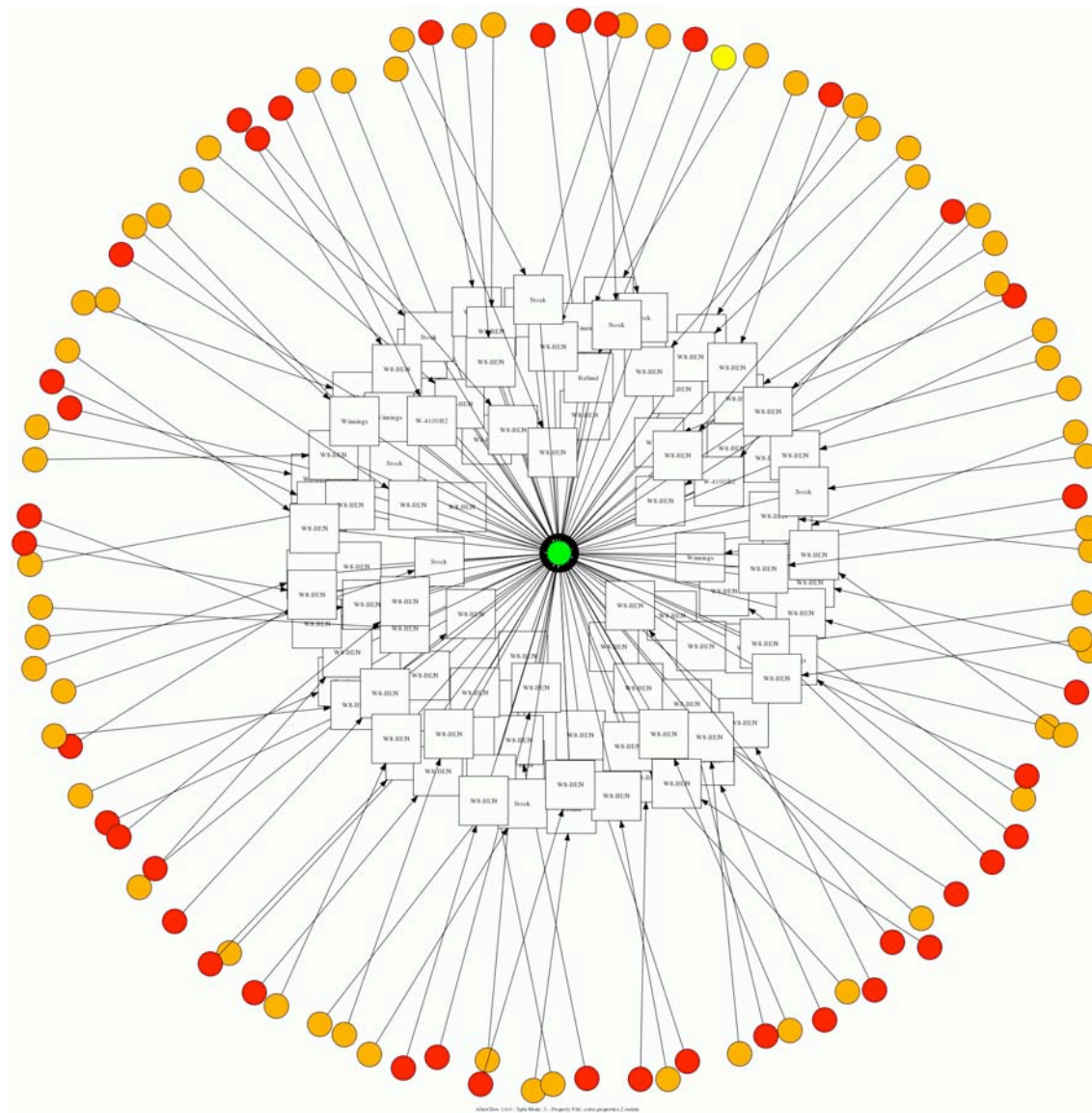
Delivery method and scam type by telco

“Who, how, and what did they
send”

- Email
- Direct Fax
- Telephone
- Telco



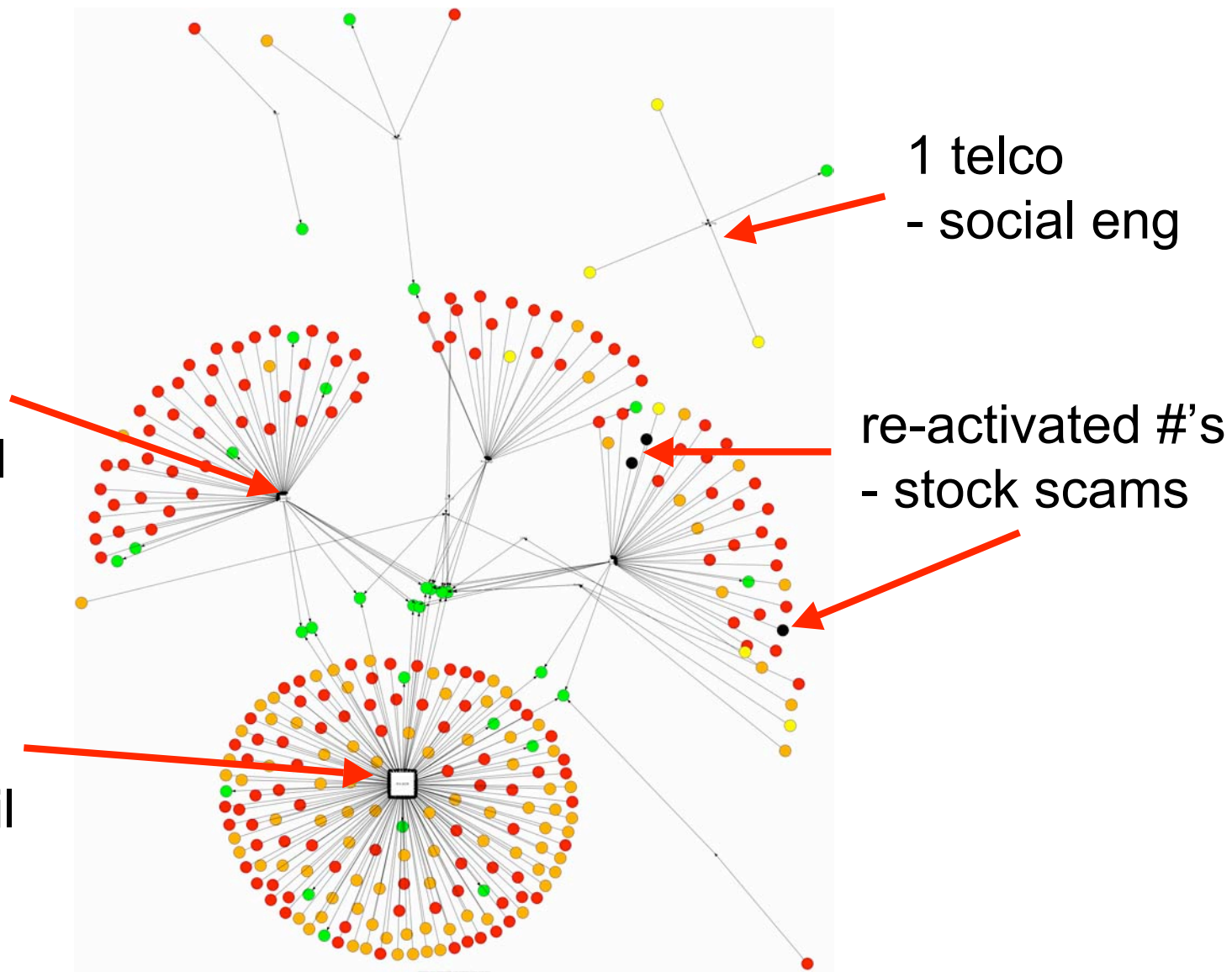
- Email
- Direct Fax
- Telephone
- Telco



- Email
- Direct Fax
- Telco
- Telephone

2 scam
- W-4100B2
- mostly email

#1 scam
- W8-BEN
- fax and email



Analysis

stock scams

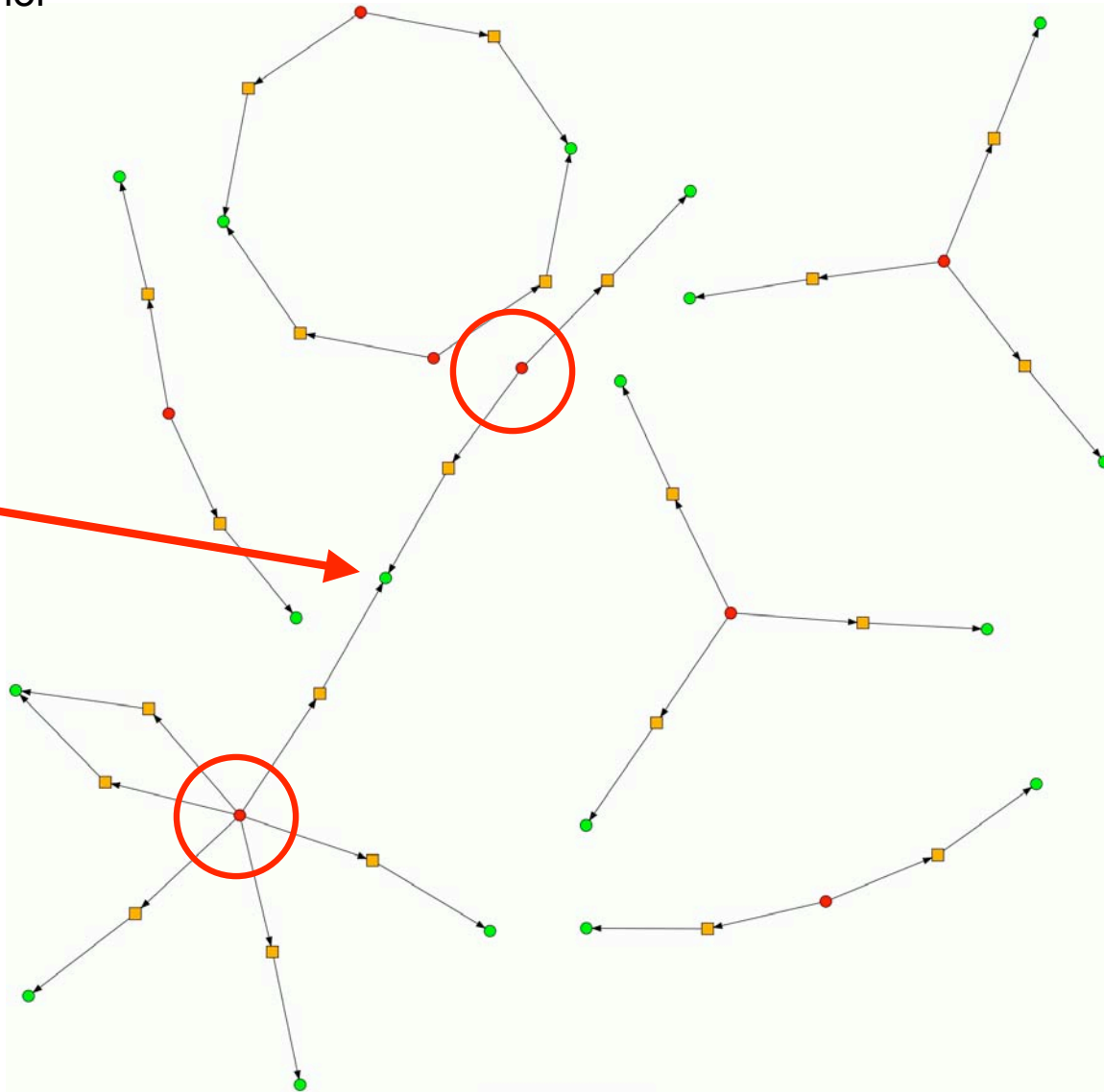
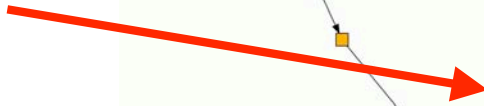
The Process

- Analyze brokerage website and metadata provided by victims
- Google unique strings (e.g., team bios, board members, etc) from fake site
 - Identify other clones
 - Identify indirect victim, the legitimate firm (i.e., the “re-skinned” website)

GOAL: determine if the stock firms share some commonality

- Stock firm
- Metadata "Author"
- Number

Two firms
share same
number

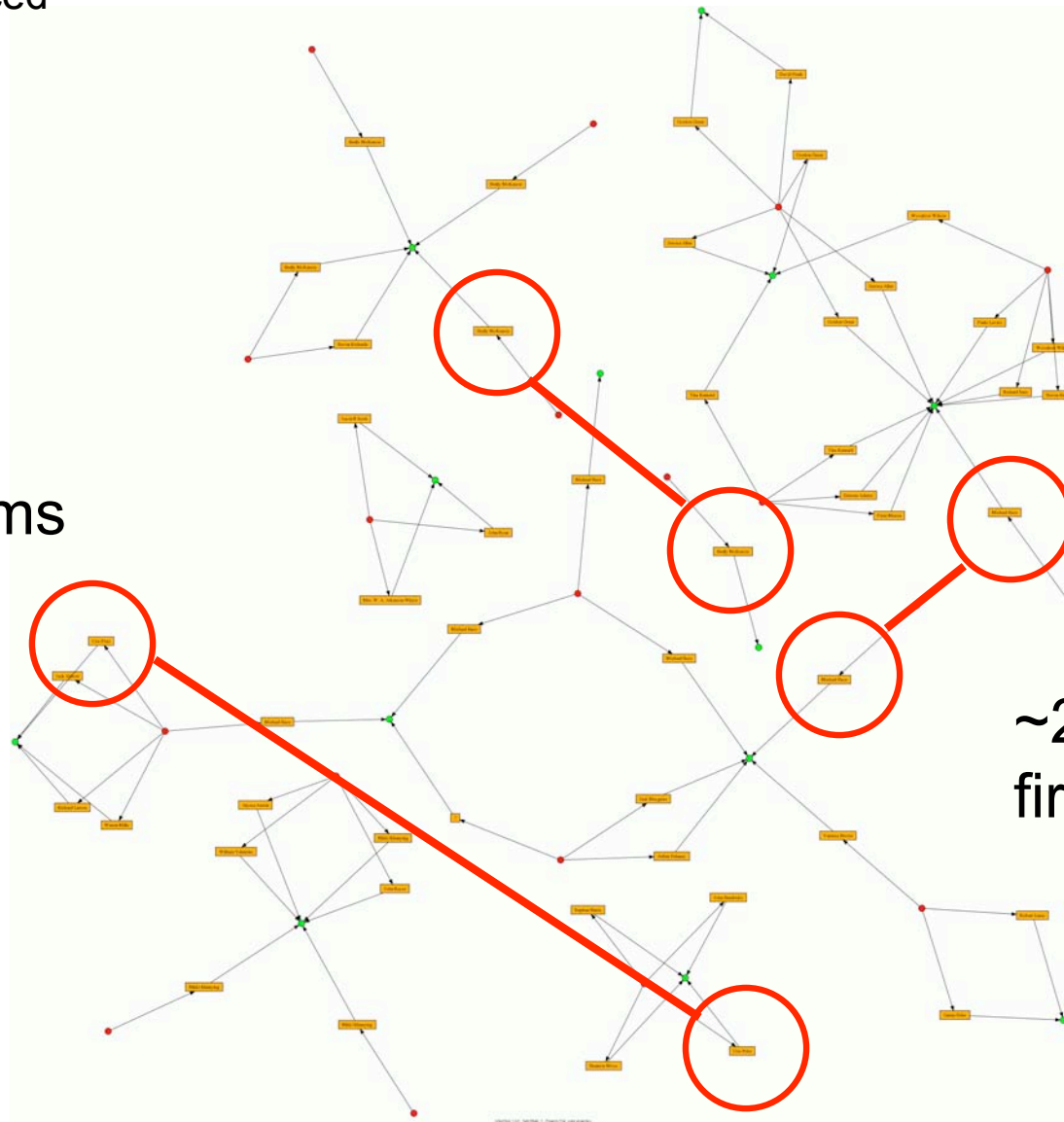


Initial Findings

- Extracted metadata from stock scams didn't yield much, expanded search
- Observed the destination of the wire transfers terminated in Philippines
- Observed similar emails and numbers across different scams

- Stock firm
- Person referenced
- Number

Same name
used in
different scams



~20 different
firms identified

Results

- Responded to victims to file complaints with FTC
- Contacted FBI, SEC, and TIGTA
- 2/3 of existing stock scams point back to Philippines

gnuplot example

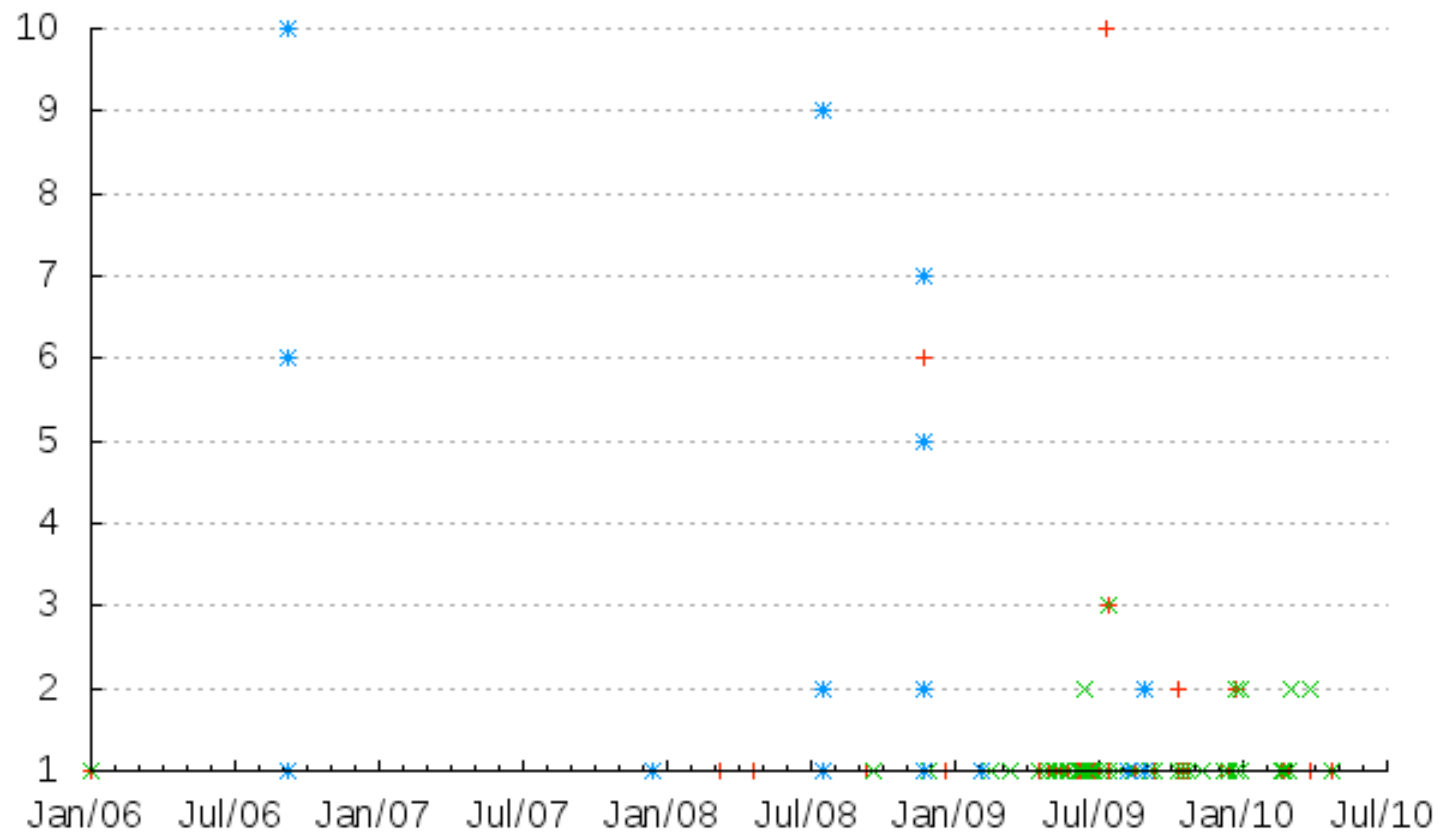
“visualization of extracted
metadata (file manipulation
date/times)”

The Process

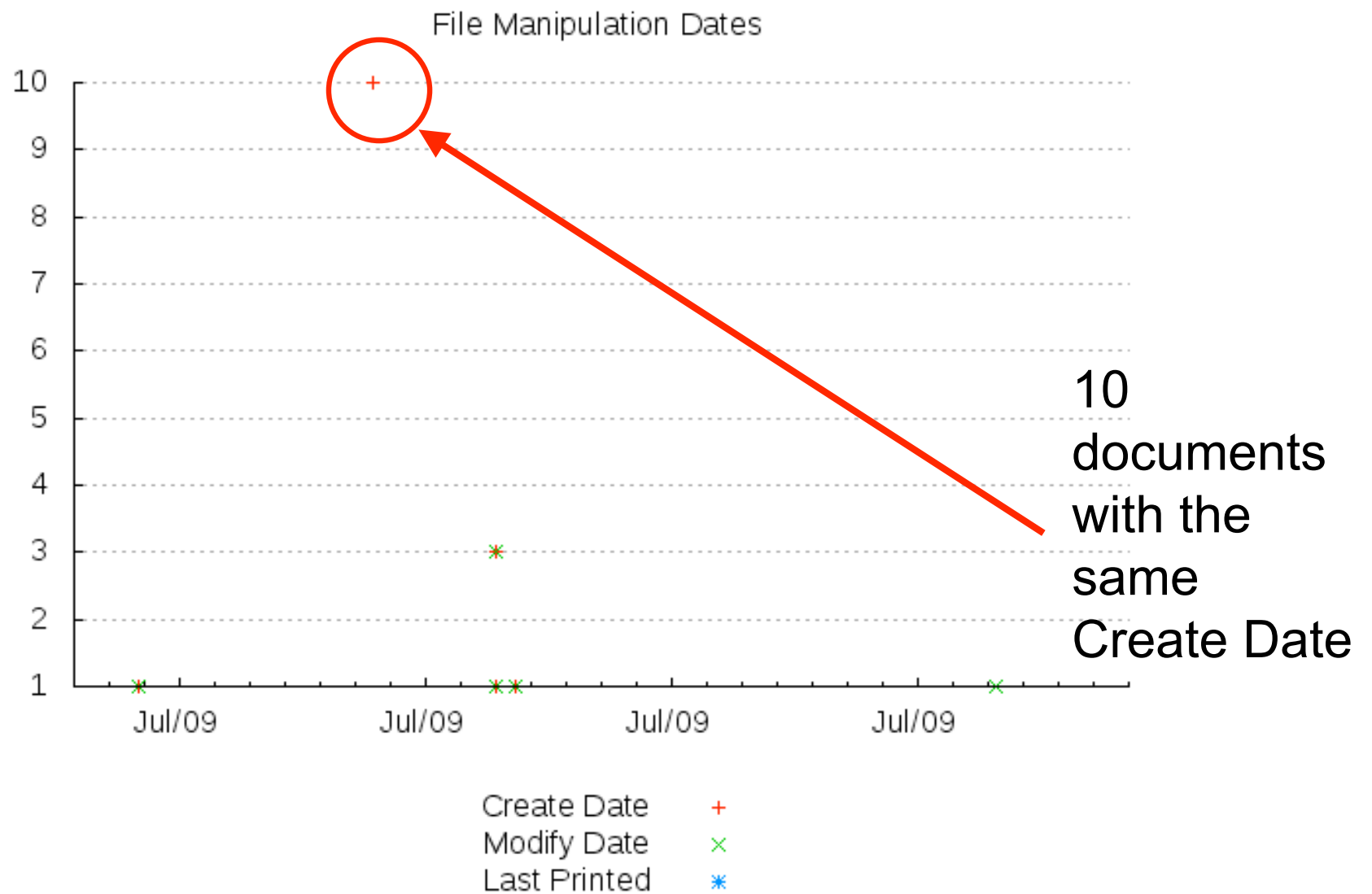
- perform historical analysis of time-series data
- plot different fields (Last Printed, Create Date, Modify Date)
- query RDBMS for that period

GOAL: determine if the numbers share some commonality

File Manipulation Dates



Create Date +
Modify Date x
Last Printed *



Results

- query database for that “Create Date”
- 10 numbers involving four carriers
- mixture of toll/toll-free numbers
- same “Last Saved By” in all incidents
- modify date positively correlates to revision number
 - as carriers disable numbers he/she edits document and sends out new one

afterglow example

“visualization of email accounts
using levenshtein distance”

Levenshtein distance

- edit distance (what is added/changed/removed) between two strings
 - “apple” -> “zebra” (edit distance = 5)
 - “apple” -> “apples” (edit distance = 1)
- applications
 - determine if a new email account closely resembles existing email accounts

The Process

1. build a hash of existing email accounts with their lev. score

TARGET EMAIL ACCT
ustreasurydept2009

2. iterate through hash to find matches \leq (string_len/2)

SAMPLE LEV DIST HASH
irs_offshore_dept25 => 13
ustreasurydepatment => 5
irs.usa => 16
ustreasurydept => 4

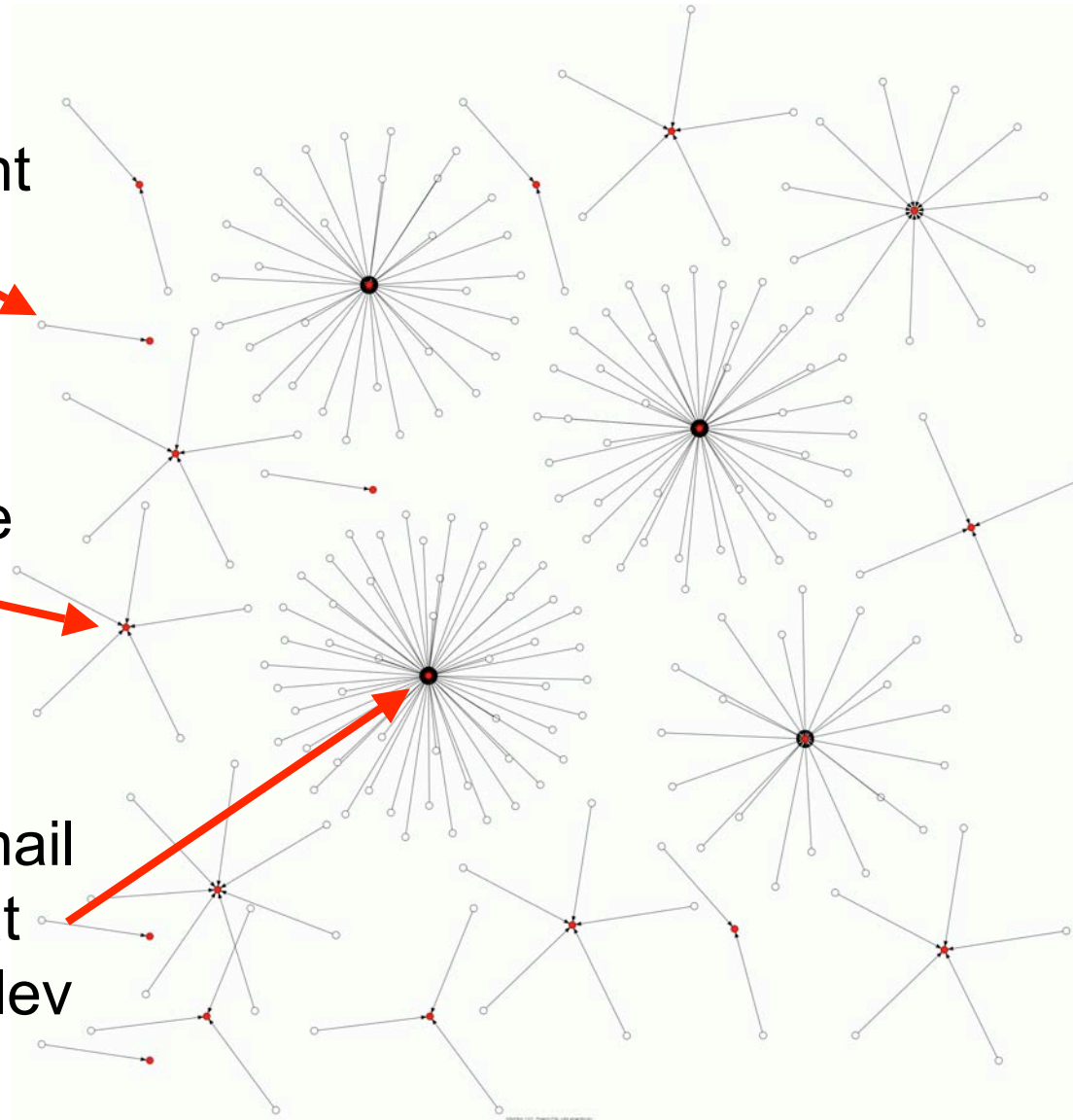
3. visualize

GOAL: find low lev dist matches

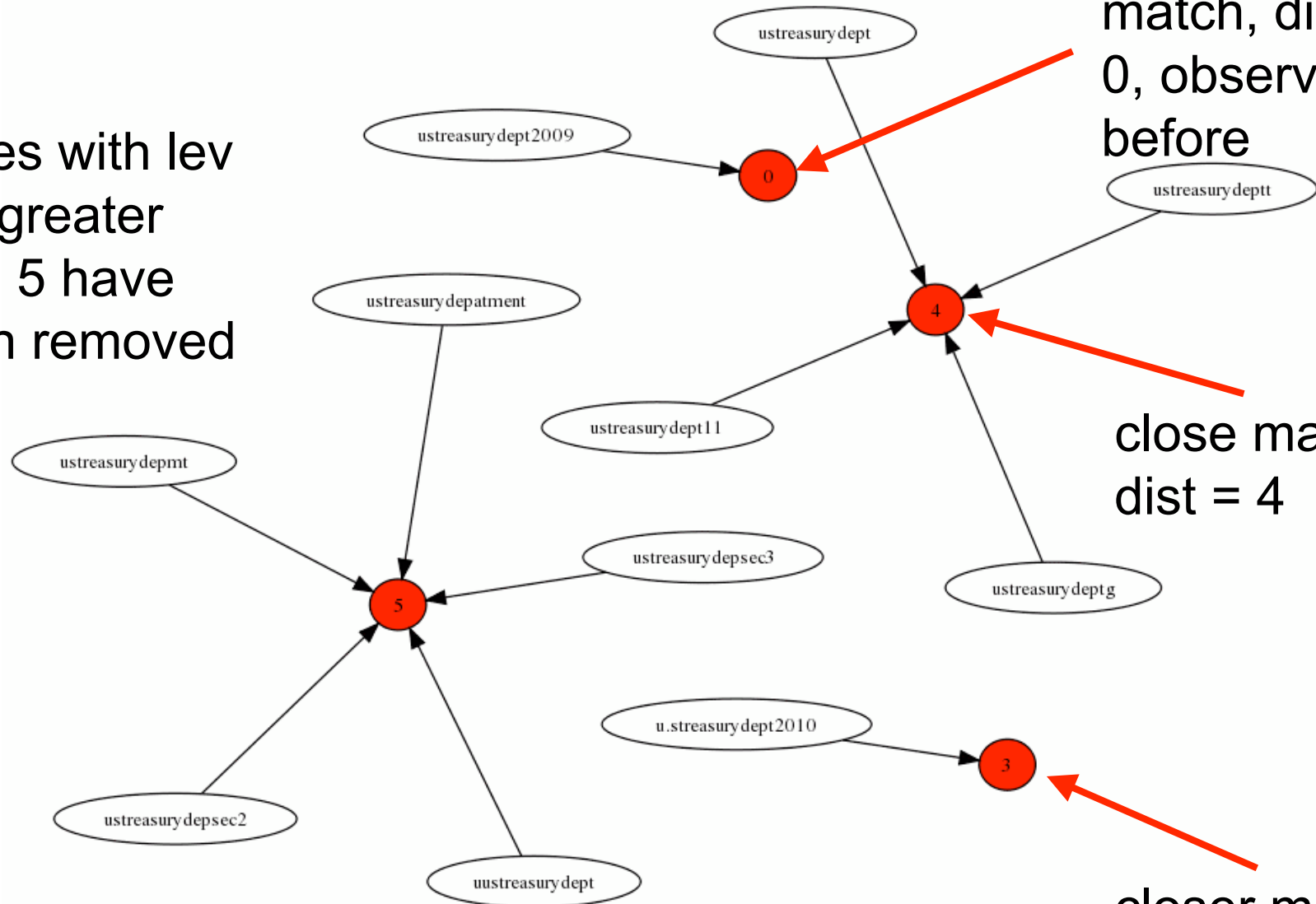
email account

lev dist score

groups of email
accounts that
share same lev
dist



nodes with lev
dist greater
than 5 have
been removed



closest
match, dist =
0, observed
before

close match,
dist = 4

closer match,
dist = 3,

Results

- Bulk of stock scams use similar email accounts
 - irs_help@
 - irs.govt.treasury@
 - irs_help.treasury@
 - treasury.help_irs@

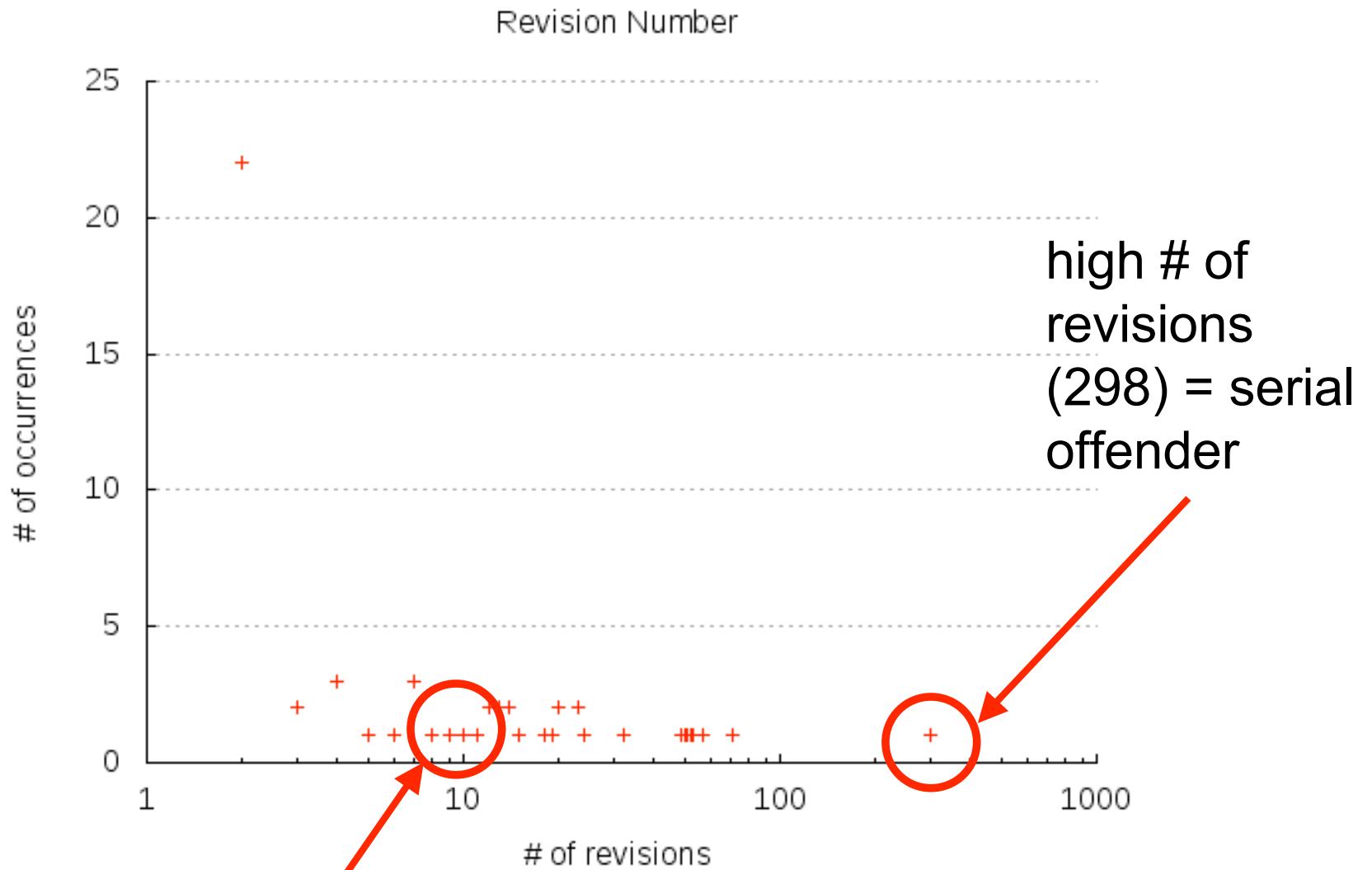
gnuplot/afterglow example

“gnuplot visualization of revision
number and afterglow
visualization of metadata”

The Process

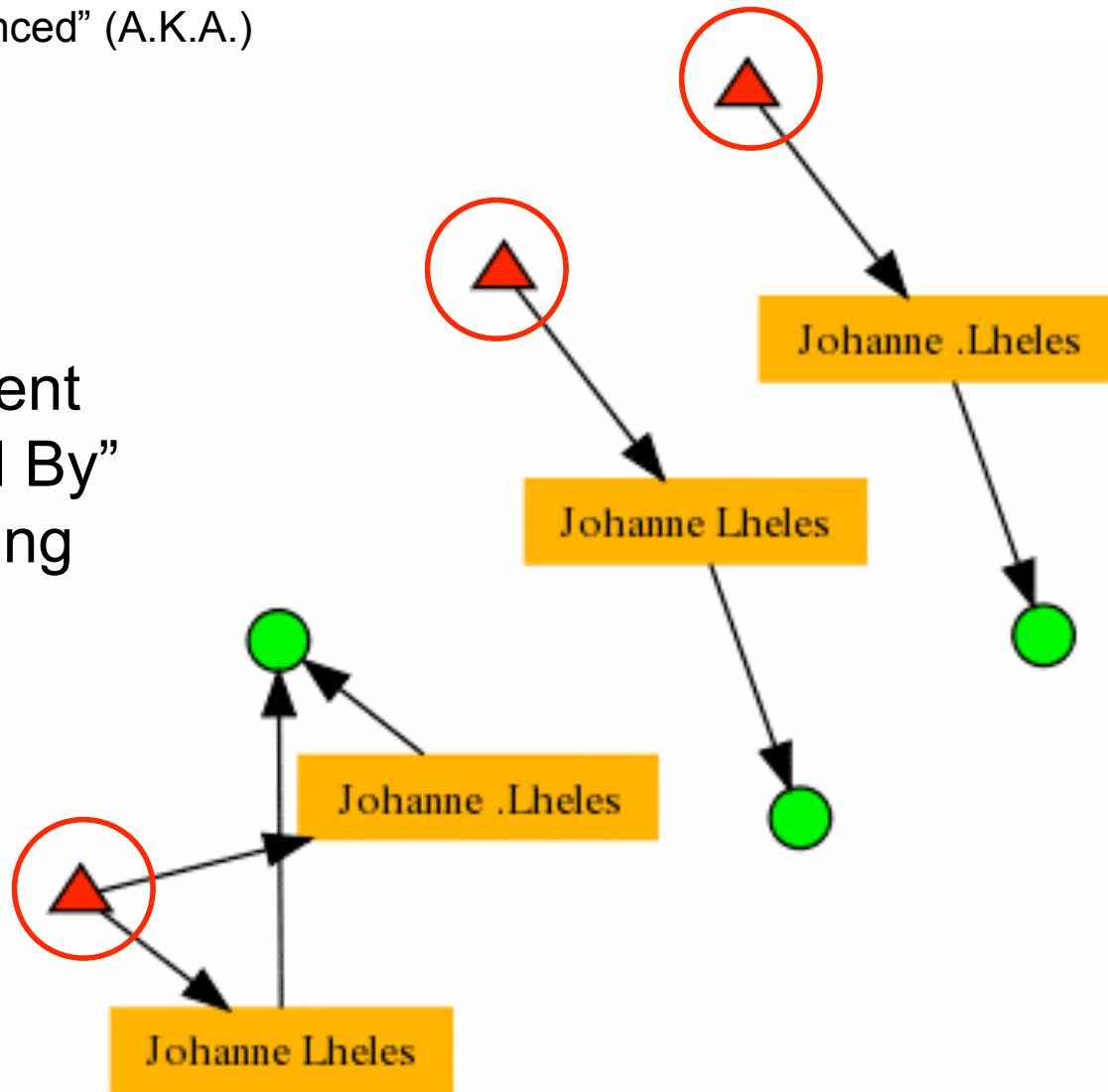
- extract “Revision Number” from database, plot using gnuplot
- look for clusters, outliers, patterns
- visualize the metadata using afterglow

GOAL: identify serial offenders



- ▲ Last Saved By
- Person referenced" (A.K.A.)
- Telco

Three different
"Last Saved By"
users all using
same alias

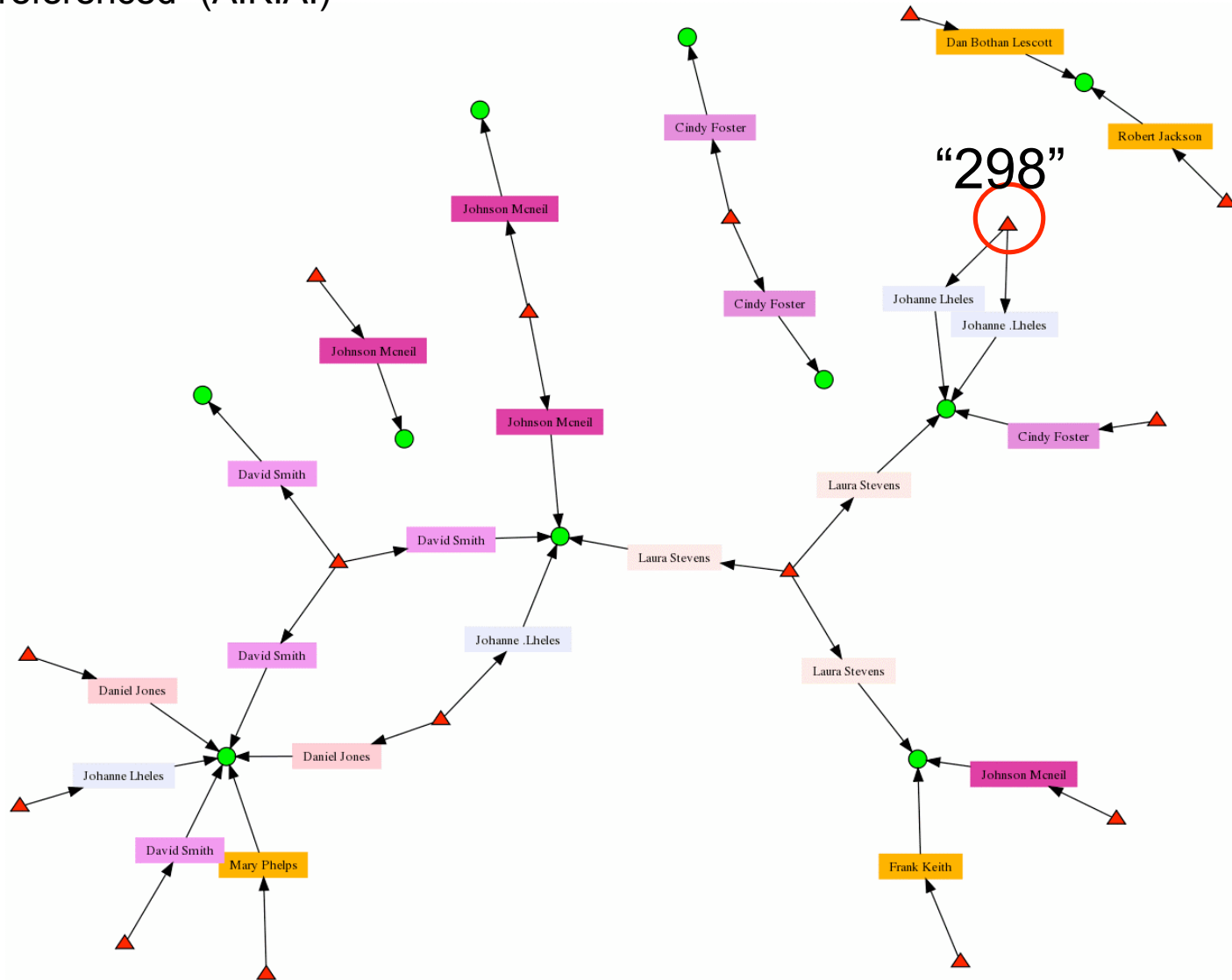


AfterGlow 1.6.0 - Split Mode: 3 - Property File: color.properties.3.group.isolate

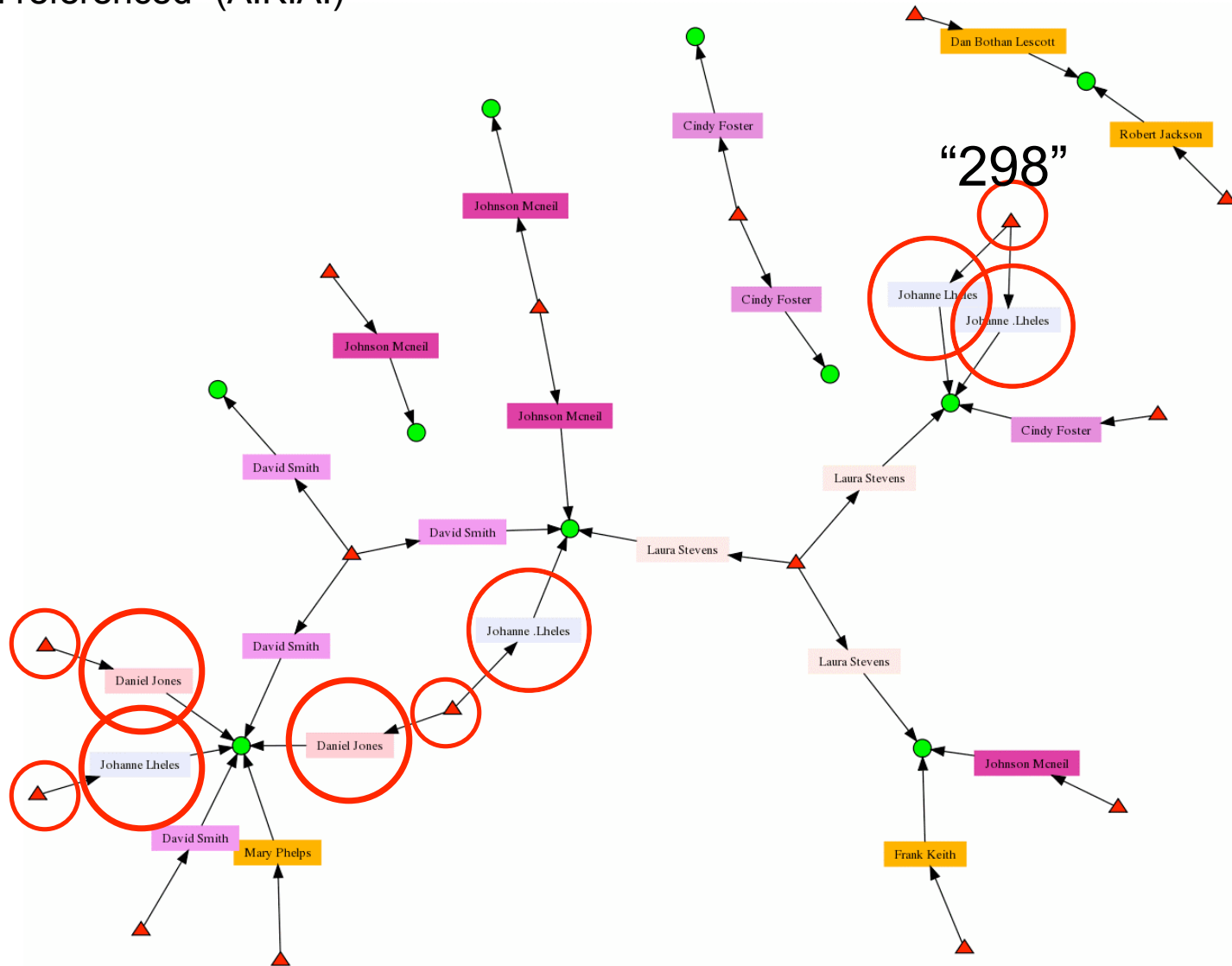
Initial Findings

- queried database for “Last Saved By” actor
- was able to show from metadata that they edit the document then resend (i.e., Revision Number increases)
- identified an alias
 - uses email as preferred delivery method
 - uses W8-BEN and W-4100B2 forms

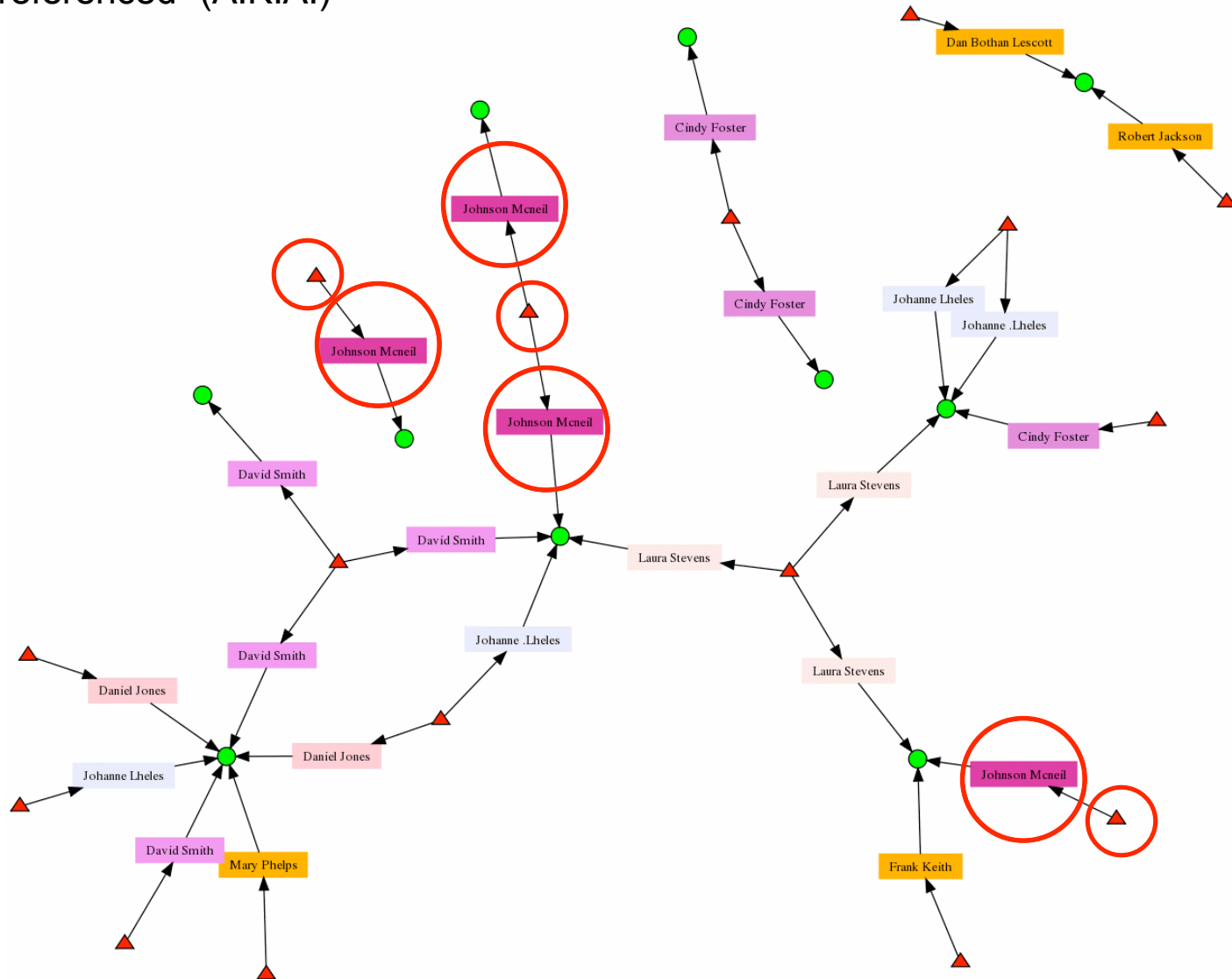
- ▲ Last Saved By
- Person referenced" (A.K.A.)
- Telco



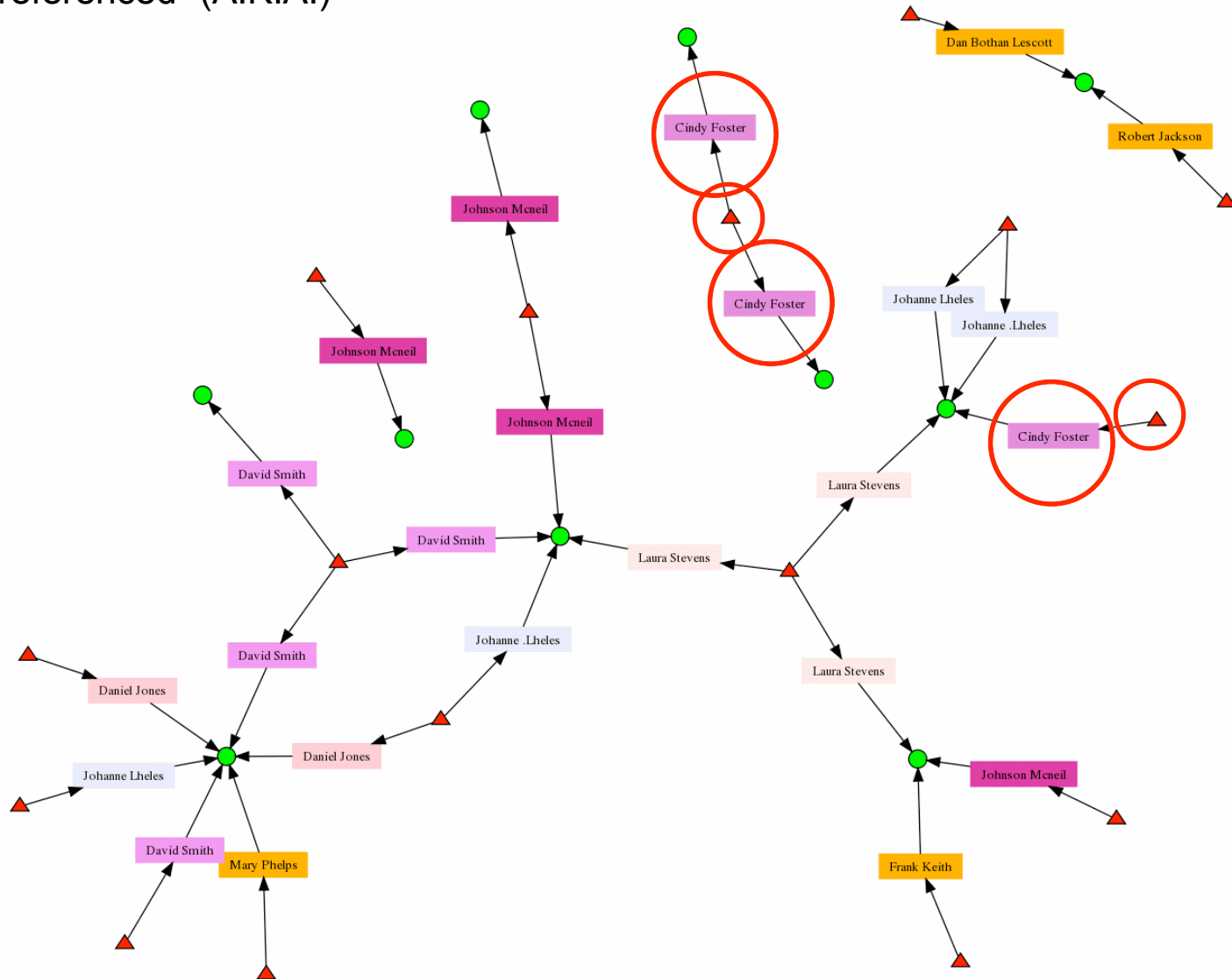
- ▲ Last Saved By
- Person referenced" (A.K.A.)
- Telco



- ▲ Last Saved By
- Person referenced" (A.K.A.)
- Telco

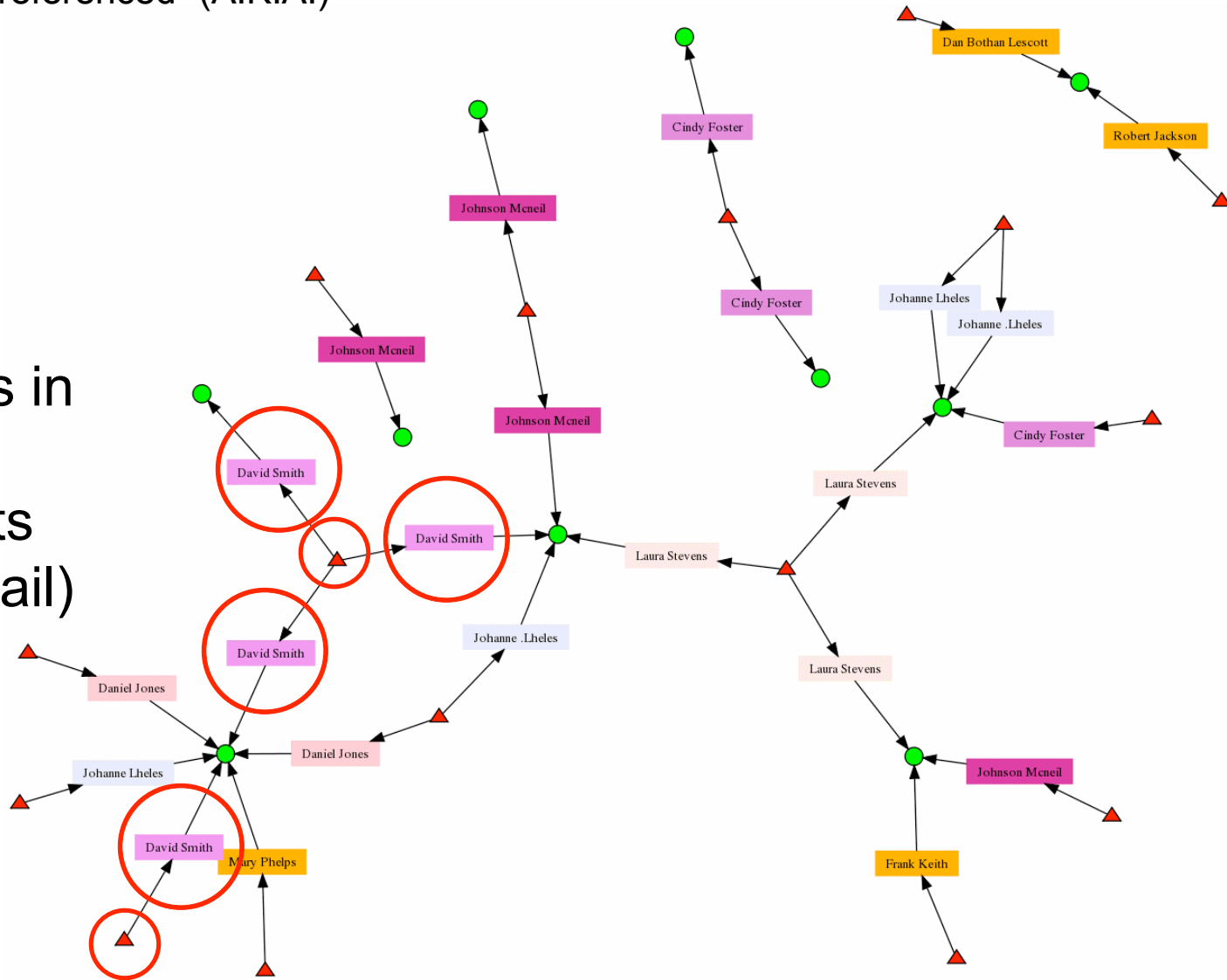


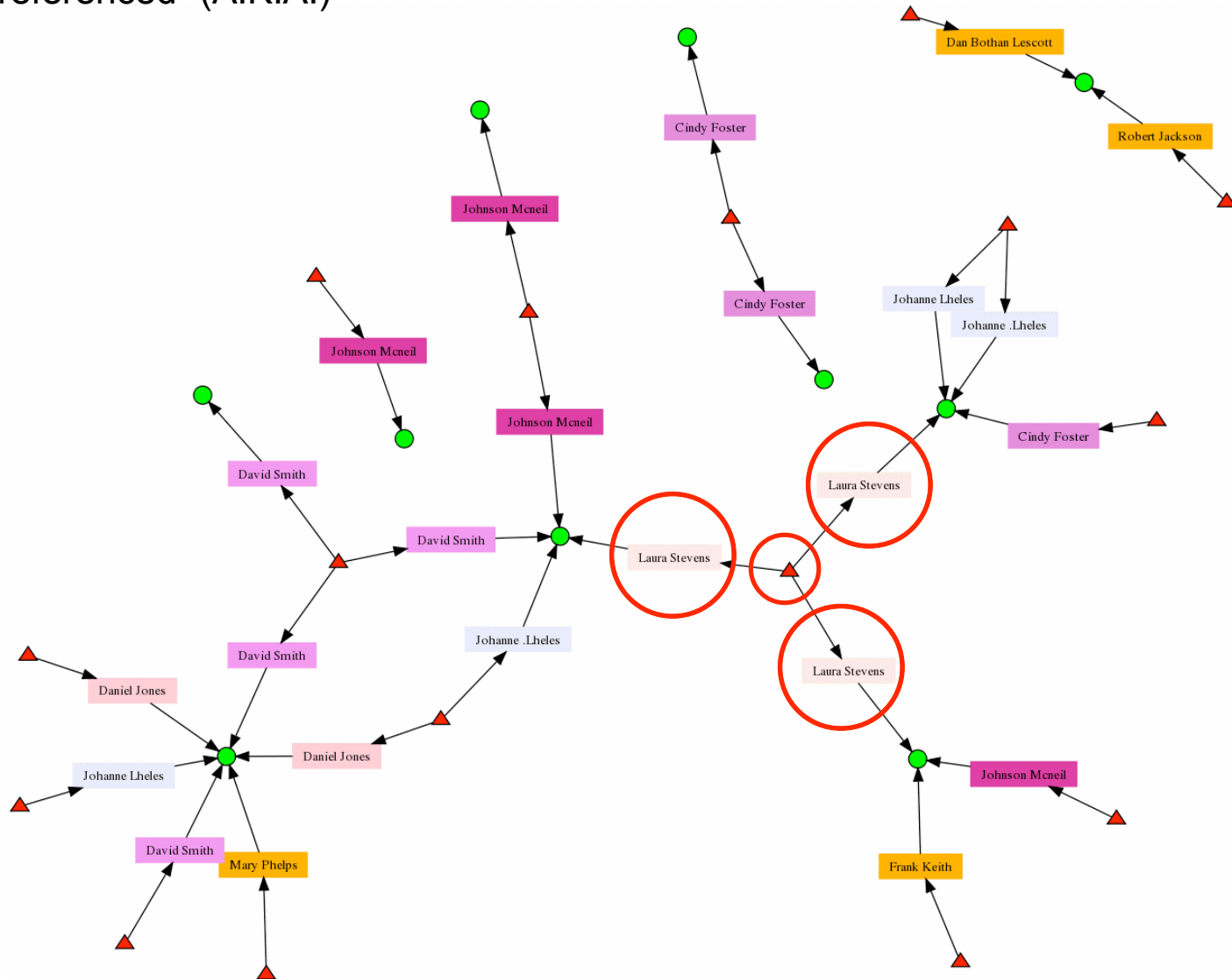
- ▲ Last Saved By
- Person referenced" (A.K.A.)
- Telco



- ▲ Last Saved By
- Person referenced" (A.K.A.)
- Telco

“David Smith” appears in 80+ incidents (fax/email)





Results

- At least 50% of all vishing incidents can be attributed to these actors based on the metadata and aliases provided
- Linking and grouping actors has allowed OFDP to assist criminal investigations

Lessons learned

- Phishers re-activate fax numbers (e.g., stock)
- W8-BEN remains most popular scam
- Same phisher will use different telcos
- A few telcos see majority of incidents
- Re-use of “person referenced” (alias) suggests shared documents/methods/groups
- Data > voice; IRS > Treasury; email > direct fax
- Majority of vishing scams disabled within 24 hours (some < 12) but some take weeks
- Phishers receive faxes directly to their email which might or might not be stored on provider’s network
- Direct faxes present a reporting problem

Recommendations (GFIRST)

- Send IRS-related phishing to phishing@irs.gov
- Mine public resources (Phishtank, Google Alerts)
- Track incidents and associated metadata if available
- Visualize metadata to reveal hidden relationships and/or groups
- Develop carriers, registrars and email service providers contacts
 - Disable phishers' telephone(s), domains, and email addresses
 - Craft an audio landing page and/or a faxback coversheet
- Leverage LE resources (US-CERT, LEAP, IC3, SMS800, NCFTA, FTC Sentinel)
- Partner with the antiphishing organizations (APWG), telco (CFCA), financial communities
- Direct individuals to:
 - <http://www.ftccomplaintassistant.gov>
 - <http://www.econsumer.gov>

Contribute to the community

- Phishtank (OpenDNS and Live Feed)
- Anti-phishing Working Group
(<http://www.apwg.org>)
- Visual Analytics Group (LinkedIn)
- SecViz (<http://www.secviz.org>)

References

- "The Visual Display of Quantitative Information" - Edward Tufte
- "Applied Security Visualization" - Raffael Marty
- "Security Data Visualization" - Greg Conti

Questions?

mark.w.henderson@irs.gov